Release Notes for Catalyst 4500 Series Software Release 7.*x*

Current Release:
7.6(17)—March 6, 2006
Previous Releases:
7.6(16), 7.6(15), 7.6(14), 7.6(13), 7.6(12), 7.6(11), 7.6(10), 7.6(9), 7.6(8), 7.6(7), 7.6(6), 7.6(5), 7.6(4), 7.6(3a), 7.6(3), 7.6(2), 7.6(1), 7.5(1), 7.4(3), 7.4(2), 7.4(1), 7.3(2), 7.3(1), 7.2(2), 7.2(1), 7.1(2a), 7.1(2), 7.1(1a), 7.1(1)

These release notes describe the features, modifications, and caveats for Catalyst 4500 series supervisor engine software release 7.*x* and all 7.*x* maintenance releases. The most current 7.*x* release is supervisor engine software release 7.6(17). These release notes apply to Catalyst 4500 series switches and Catalyst 2948G, 4912G, and 2980G-A switches running Catalyst 4500 series supervisor engine software. We recommend that you read these release notes before using your switch or upgrading your switch software.

Note For the most recent information on open caveats, refer to the most current version of these release notes at this URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/relnotes/ol_1983.htm

Caution To avoid losing all or part of the configuration stored in NVRAM, always back up the switch configuration file before upgrading or downgrading the switch software. A software downgrade will always cause the configuration to be lost. Use the **copy config tftp** command to back up your configuration to a TFTP server. Use the **copy config flash** command to back up the configuration to a Flash device.

Contents

This document consists of these sections:

- System Requirements, page 3
- Product and Software Release Support Matrix, page 9
- Release 7.x Orderable Software Images, page 12

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2006 Cisco Systems, Inc. All rights reserved.

- New Features for Supervisor Engine Software Release 7.6, page 14
- New Features for Supervisor Engine Software Release 7.5, page 14
- New Features for Supervisor Engine Software Release 7.4, page 15
- New Features for Supervisor Engine Software Release 7.3, page 16
- New Features for Supervisor Engine Software Release 7.2, page 16
- New Features for Supervisor Engine Software Release 7.1, page 17
- Open and Resolved Caveats in Software Release 7.6(17), page 18
- Open and Resolved Caveats in Software Release 7.6(16), page 19
- Open and Resolved Caveats in Software Release 7.6(15), page 19
- Open and Resolved Caveats in Software Release 7.6(14), page 20
- Open and Resolved Caveats in Software Release 7.6(13), page 20
- Open and Resolved Caveats in Software Release 7.6(12), page 21
- Open and Resolved Caveats in Software Release 7.6(11), page 22
- Open and Resolved Caveats in Software Release 7.6(10), page 23
- Open and Resolved Caveats in Software Release 7.6(9), page 24
- Open and Resolved Caveats in Software Release 7.6(8), page 26
- Open and Resolved Caveats in Software Release 7.6(7), page 28
- Open and Resolved Caveats in Software Release 7.6(6), page 28
- Open and Resolved Caveats in Software Release 7.6(5), page 30
- Open and Resolved Caveats in Software Release 7.6(4), page 31
- Open and Resolved Caveats in Software Release 7.6(3a), page 32
- Open and Resolved Caveats in Software Release 7.6(3), page 33
- Open and Resolved Caveats in Software Release 7.6(2), page 34
- Open and Resolved Caveats in Software Release 7.6(1), page 35
- Open and Resolved Caveats in Software Release 7.5(1), page 38
- Open and Resolved Caveats in Software Release 7.4(3), page 39
- Open and Resolved Caveats in Software Release 7.4(2), page 39
- Open and Resolved Caveats in Software Release 7.4(1), page 40
- Open and Resolved Caveats in Software Release 7.3(1), page 41
- Open and Resolved Caveats in Software Release 7.2(2), page 43
- Open and Resolved Caveats in Software Release 7.2(1), page 44
- Open and Resolved Caveats in Software Release 7.1(2a), page 47
- Open and Resolved Caveats in Software Release 7.1(2), page 48
- Open and Resolved Caveats in Software Release 7.1(1a), page 49
- Open and Resolved Caveats in Software Release 7.1(1), page 50
- Usage Guidelines, Restrictions, and Troubleshooting, page 51
- Software Documentation Updates for Release 7.1, page 61
- Related Documentation, page 61

- Obtaining Documentation, page 62
- Obtaining Technical Assistance, page 63
- Obtaining Additional Publications and Information, page 64

System Requirements

These sections describe the system requirements for the Catalyst 4500 series switches:

- Power Supply Requirements, page 3
- Release 7.x Memory Requirements, page 3
- ROMMON Requirements, page 3
- Upgrading the ROMMON, page 3
- Migrating Supervisor Engine II from a Catalyst 4006 Switch to a Catalyst 4500 Series Switch, page 7

Power Supply Requirements

The Catalyst 4006 switch requires dual power supplies. The Catalyst 4500 series switch requires one power supply (dual for redundancy).

Release 7.*x* Memory Requirements

The Catalyst 4500 series supervisor engine software release 7.*x* requires a minimum of 64-MB DRAM installed on your supervisor engine. All Supervisor Engine II modules are shipped with 64-MB DRAM.

If your Supervisor Engine I has less than 64-MB DRAM, you can add more memory by ordering the 32-MB DRAM upgrade (Cisco product number MEM-C4K-32-RAM=) for the Catalyst 4500 series Supervisor Engine I.

ROMMON Requirements

If the Boot ROM (ROMMON) loaded onto your switch is version 4.5(1) or earlier, you need to upgrade the ROMMON to at least version 5.4(1) in order to run software release 7.1 or later.

Upgrading the ROMMON

Follow these guidelines to upgrade the ROMMON on your switch:

Caution To avoid actions that might make your system unbootable, read this entire section before starting the upgrade.

You can perform this procedure entirely over a Telnet connection, but if something fails, you will need to have access to the console serial port. If done improperly, the system can become unbootable, and you will have to return it to Cisco for repair.

This section describes an upgrade to ROMMON version 6.4(1). The same procedure applies to other ROMMON versions, but you will have to substitute appropriate version numbers in the upgrade image names.

Step 1 Download the **promupgrade** program from Cisco.com, and place it on a TFTP server in a directory that is accessible from the switch to be upgraded.

The **promupgrade** programs are available at the same location on Cisco.com where you download Catalyst 4500 series system images.

To upgrade to ROMMON version 6.1(4), download the **cat4000-promupgrade.6-1-4.bin** file.

Step 2 In privileged mode on your switch, use the **show version** command to verify the ROMMON version loaded on the switch.

The ROMMON version number is listed as the System Bootstrap Version. For example, in this output, the system is running ROMMON version 6.1(2):

```
Console> (enable) show version
WS-C4003 Software, Version NmpSW:5.5(8)
Copyright (c) 1995-2001 by Cisco Systems, Inc.
NMP S/W compiled on May 24 2001, 21:12:09
GSP S/W compiled on May 24 2001, 18:39:50

System Bootstrap Version:6.1(2)

Hardware Version:1.0  Model:WS-C4003  Serial #:xxxxxxxxx

.
.
.
Console > (enable)
```

Step 3 Use the **dir bootflash:** command to ensure that there is sufficient space in Flash memory to store the **promupgrade** image. If there is insufficient space, delete one or more images, and then enter the **squeeze bootflash:** command to reclaim the space.

Step 4 Download the **promupgrade** image into Flash memory using the **copy tftp** command.

This example shows how to download the **promupgrade** image **cat4000-promupgrade.6-1-4.bin** from the remote host **Lab_Server** to bootflash:

```
Console> (enable) copy tftp flash
IP address or name of remote host []? Lab_Server
Name of file to copy from []? /cat4000-promupgrade.6-1-4.bin
Flash device []? bootflash
Name of file to copy to []? cat4000-promupgrade.6-1-4.bin

9205592 bytes available on device bootflash, proceed (y/n) [n]? y
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
File has been copied successfully.
Console > (enable)
```

Step 5 Ensure that the last line in the output of the **show boot** command is `boot:image specified by the boot system commands.`

- If the last line in the output of the **show boot** command is not `boot:image specified by the boot system commands`, go to Step 6.
- If the last line in the output of the **show boot** command is `boot:image specified by the boot system commands`, go to Step 7.

This example shows the autoboot configuration:

```
Console> (enable) show boot
BOOT variable = bootflash:cat4000.5-5-8.bin,1;
CONFIG_FILE variable = bootflash:switch.cfg

Configuration register is 0x102
ignore-config:disabled
auto-config:non-recurring
console baud:9600
→ boot:image specified by the boot system commands
Console > (enable)
```

Step 6 If the last line in the output of the **show boot** command is not `boot:image specified by the boot system commands`, use the **set boot config-register** command to set the boot configuration.

This example shows how to set the boot configuration:

```
Console > (enable) set boot config-register boot system
Configuration register is 0x102
ignore-config:disabled
auto-config:non-recurring
console baud:9600
boot:image specified by the boot system commands
Console > (enable)
```

Step 7 Use the **set boot system flash** command to prepend the **promupgrade** image to the boot string.

Note Make sure that you use the **prepend** keyword with the **set boot system flash** command. The switch always boots the first image in the boot string, and you want the **promupgrade** image to boot first.

This example shows how to prepend the **promupgrade** image to the boot string:

```
Console> (enable) set boot system flash bootflash:cat4000-promupgrade.6-1-4.bin prepend
BOOT variable = bootflash:cat4000-promupgrade.6-1-4.bin,1;bootflash:cat4000.5-5-8.bin,1;
```

Step 8 Reset the switch to boot the **promupgrade** program.

Caution No intervention is necessary to complete the upgrade. Do **not** interrupt the boot process by performing a reset, power cycle, OIR of the supervisor engine, etc. for at least five minutes! If the process is not allowed to complete, you may damage the switch and have to return it to Cisco for repair.

Upgrading the ROMMON may require up to 5 minutes because the switch boots the **promupgrade** image. This special program erases the current ROMMON from Flash memory and installs the new one. After installing the new ROMMON, the system resets again and boots the next image in the BOOT string. If the BOOT string was configured as described in Step 7 on page 5, the next image is the software image that the switch was originally configured to boot.

Note A Telnet session is disconnected when you reset the switch; you will lose connectivity to the switch for approximately one minute.

If you are connected to the console serial port, output similar to the following is displayed after you reset the switch:

```
0:00.530901:ig0:00:10:7b:aa:d3:fe is 172.20.59.203
0:00.531660:netmask:255.255.255.0
```

```
0:00.532030:broadcast:172.20.59.255
0:00.532390:gateway:172.20.59.1
WS-X4012 bootrom version 6.1(2), built on 2000.04.03 15:20:09
H/W Revisions:Meteor:2 Comet:8 Board:1
Supervisor MAC addresses:00:10:7b:aa:d0:00 through 00:10:7b:aa:d3:ff (1024 addresses)
Installed memory:64 MB
Testing LEDs.... done!
The system will autoboot in 5 seconds.
Type control-C to prevent autobooting.
rommon 1 >
The system will now begin autobooting.
Autobooting image:
"bootflash:cat4000-promupgrade.6-1-4.bin"

CCCC
```

```
Hardware Version:1.0  Model:WS-C4003  Serial #:xxxxxxxxx

.
.
.
Console > (enable)
```

Caution When entering the **clear boot system flash cat.4000-promupgrade.6-1-4.bin** command, be sure to type the correct **promupgrade** image in the command syntax. If you enter only **clear boot system flash**, all images in the autoboot string are cleared, and the switch will not know which image to boot.

Step 10 Use the **clear boot system flash** *promupgrade_image* command to remove the **promupgrade** program from the autoboot string.

This example shows how to remove the **promupgrade** image **cat.4000-promupgrade.6-1-4.bin** from the boot sequence. Notice that the response message shows the system image for software release 5.5(8) in the autoboot string:

```
Console> (enable) clear boot system flash bootflash:cat4000-promupgrade.6-1-4.bin
BOOT variable = bootflash:cat4000.5-5-8.bin,1;
```

Step 11 Use the **del** command to delete the **promupgrade** program from the Flash memory and squeeze the Flash memory to reclaim unused space.

This example shows how to delete the **promupgrade** image **cat.4000-promupgrade.6-1-4.bin** from the Flash memory and reclaim unused space:

```
Console> (enable) del bootflash:cat4000-promupgrade.6-1-4.bin
Console> (enable) squeeze bootflash:

All deleted files will be removed, proceed (y/n) [n]? y

Squeeze operation may take some time, proceed (y/n) [n]? y
Console > (enable)
```

Step 12 After removing the **promupgrade** image from the BOOT string, use the **show boot** command to verify that the BOOT string is set correctly.

Migrating Supervisor Engine II from a Catalyst 4006 Switch to a Catalyst 4500 Series Switch

If you migrate your Supervisor Engine II from a Catalyst 4006 switch to a Catalyst 4503 or 4506 switch, save your configuration and reload the configuration file after you insert the supervisor engine into the Catalyst 4500 series chassis.

The Catalyst 4500 series switch requires software release 7.4(1) or a later release. If your Supervisor Engine II is running software release 7.3(2) or an earlier release, upgrade to software release 7.4(1) or a later release before migrating your supervisor engine to a Catalyst 4500 series chassis.

Caution If you attempt to boot a Supervisor Engine II running software release 7.3(2) or an earlier release in a Catalyst 4500 series chassis, the switch will continuously reboot.

If the switch continuously reboots, you need to do one of the following:

- Reinsert the supervisor engine into the Catalyst 4006 switch, and load software release 7.4(1) or a later release, and then migrate the supervisor engine to the Catalyst 4500 series chassis.
- Access ROMMON mode while the supervisor engine is in the Catalyst 4500 series switch, and load the 7.4(1) image from ROMMON. For more information, refer to this publication: http://www.cisco.com/warp/public/473/26.html

The Catalyst 4006 switch has 1024 MAC addresses that can be used as bridge identifiers; the Catalyst 4500 series switches have 64 MAC addresses. MAC address reduction is always enabled on the Catalyst 4500 series switches; however, it may or may not be enabled on the Catalyst 4006 switch. Whether or not MAC address reduction is enabled might affect the selection of the root bridge after you migrate your supervisor engine. Here are two scenarios to consider:

- The Catalyst 4006 switch is not a root switch

  In this case, the spanning tree topology does not change. If you add a Catalyst 4500 series switch with MAC reduction enabled to the network and its default spanning tree bridge ID priority is set to 32,768, the bridge ID priority of the new switch becomes the bridge ID priority that is added to a system ID extension. The system ID extension is the VLAN number and can range from 1 to 4094. If the switch is in VLAN 1, the new bridge ID priority will be 32,789. Because 32,769 is greater than 32,768, this switch cannot become the root switch.

- The Catalyst 4006 is a root switch

  In this case, the spanning tree topology may change. If the other switches in the network are not running MAC address reduction, the topology will change after you replace the chassis with a Catalyst 4500 series switch. The bridge ID priority of the new Catalyst 4500 series switch increments in the same manner as in the previous scenario (bridge ID priority + VLAN number). If the switch is in VLAN 1, the new bridge ID will be 32,789. Because 32,769 is greater than 32,768, this switch cannot become the root switch. The network designates a new root switch; the spanning tree topology also changes to reflect the new root switch.

  If the bridge priority of the Catalyst 4006 has been lowered administratively and you use the same configuration in the new Catalyst 4500 series switch, then the switch remains the root switch and the spanning tree topology does not change.

Before migrating your supervisor engine from a Catalyst 4006 switch to a Catalyst 4503 or 4506 switch, make sure that the supervisor engine is running software release 7.4(1). If your switch is running software release 7.3(2) or an earlier release, upgrade to software release 7.4(1) or a later release. For more information, refer to Chapter 23, “Working with System Software Images,” in the *Software Configuration Guide*. To migrate your supervisor engine from a Catalyst 4006 switch to a Catalyst 4503 or 4506 switch, perform this task:

	Task	Command
Step 1	Change the nondefault configuration mode to text, and specify the configuration file to use at boot up.	**set config mode text bootflash:switch.cfg**
Step 2	Save the current nondefault configuration to NVRAM.	**write memory**
Step 3	Save the configuration on the Catalyst 4006 switch.	**copy config flash**
Step 4	Remove the supervisor engine from the Catalyst 4006 switch, and insert it into the Catalyst 4500 series switch.	–

	Task	Command
Step 5	Clear the current configuration.	**clear config all**
Step 6	Load the saved configuration.	**configure bootflash:switch.cfg**
Step 7	If you have only one power supply in your Catalyst 4506 switch, set the power budget to 1.	**set power budget 1**

Product and Software Release Support Matrix

This section contains configuration matrixes to help you order Catalyst 4500 series products. Table 1 lists the minimum supervisor engine software release and the current recommended supervisor engine software release for Catalyst 4500 series modules and chassis.

Table 1 Product and Supervisor Engine Software Version Matrix

Product Number (append with "=" indicates spares)	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
Supervisor Engine			
WS-X4012	Catalyst 4000 series Supervisor Engine I	4.5(8)	7.4(3)
WS-X4013	Catalyst 4000 series Supervisor Engine II, 2 GBIC ports, console port (RJ-45), management port (RJ-45)	5.4(2) for Catalyst 4000 series chassis 7.4(1) for Catalyst 4500 series chassis	7.4(3)
Ethernet, Fast Ethernet, and Gigabit Ethernet			
WS-X4148-RJ	48-port 10/100 Fast Ethernet RJ-45	4.5(8)	7.4(3)
WS-X4232-GB-RJ	32-port 10/100 Fast Ethernet RJ-45, plus 2-port 1000BASE-X (GBIC) Gigabit Ethernet		
WS-X4232-L3	32-port 10/100 Fast Ethernet RJ-45 plus 2 full-duplex 1000BASE-X (GBIC) Gigabit Ethernet Layer 3 module	5.5(1)	7.4(3)
WS-X4148-RJ45V	48-port inline power 10/100BASE-TX switching module	6.1(1)	7.4(3)
WS-X4232-RJ-XX	32-port 10/100 Fast Ethernet RJ-45	5.1(1)	7.4(3)
WS-X4306-GB	6-port 1000BASE-X (GBIC) Gigabit Ethernet	4.5(8)	7.4(3)
WS-X4418-GB	18-port 1000BASE-X (GBIC) Gigabit Ethernet switching module	4.5(8)	7.4(3)
WS-X4412-2GB-T	12-port 1000BASE-T Gigabit Ethernet switching module	5.4(2)	7.4(3)
WS-X4124-FX-MT	24-port 100BASE-FX Fast Ethernet switching module	5.4(2)	7.4(3)
WS-X4148-RJ21	48-port 10/100-Mbps Fast Ethernet switching module	5.4(2)	7.4(3)

Table 1 Product and Supervisor Engine Software Version Matrix (continued)

Product Number (append with "=" indicates spares)	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-X4148-FX-MT	48-port 100BASE-FX Fast Ethernet switching module	6.2(1)	7.4(3)
WS-X4424-GB-RJ45	24-port 10/100/1000BASE-T Gigabit Ethernet switching module	6.3(1)	7.4(3)
WS-X4448-GB-LX	48-port Gigabit Ethernet switching module	6.3(1)	7.4(3)
WS-X4448-GB-RJ45	48-port Gigabit Ethernet switching module	7.1(1a)	7.4(3)
Uplink Modules			
WS-U4504-FX-MT	4-port 100BASE-FX MT-RJ	5.1(1)	7.4(3)
Gigabit Interface Converters (GBICs)			
WS-G5484=	1000BASE-SX GBIC	4.5(8)	7.4(3)
WS-G5486=	1000BASE-LX/LH GBIC		
WS-G5487=	1000BASE-ZX GBIC	4.5(8)	7.4(3)
WS-G5483=	1000BASE-TX GBIC	7.2(1)	7.4(3)
CWDM-GBIC-1470= CWDM-GBIC-1490= CWDM-GBIC-1510= CWDM-GBIC-1530= CWDM-GBIC-1550= CWDM-GBIC-1570= CWDM-GBIC-1590= CWDM-GBIC-1610=	1000BASE-X GBIC	7.2(1)	7.4(3)
Modular Chassis			
WS-C4003-S1	Catalyst 4003 chassis (3 slot)	4.5(8))	7.4(3)
WS-C4006-S2	Catalyst 4006 chassis (6 slot)	5.4(2)	7.4(3)
WS-C4503	Catalyst 4503 chassis (3 slot), fan, no power supply	7.4(1)	7.4(3)
WS-C4506	Catalyst 4506 chassis (6 slot), fan, no power supply	7.4(1)	7.4(3)
Fixed-Configuration Chassis			
WS-C2948G	Catalyst 2948G with 2 1000BASE-X (GBIC) Gigabit Ethernet uplinks and 48 10/100 Fast Ethernet ports	4.5(8)	7.4(3)
WS-C4912G	Catalyst 4912G with 12 1000BASE-X (GBIC) Gigabit Ethernet ports	4.5(8)	7.4(3)
WS-C2980G	Catalyst 2980G with 80 10/100 Fast Ethernet ports and 2 1000BASE-X ports	5.4(2)	7.4(3)
WS-C2980G-A	Catalyst 2980G-A with 80 10/100 Fast Ethernet ports and 2 1000BASE-X ports	6.1(1)	7.4(3)

Table 1 Product and Supervisor Engine Software Version Matrix (continued)

Product Number (append with "=" indicates spares)	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
Power Supplies			
WS-X4008=	400 W AC Power Supply for Catalyst 4000 series chassis	4.5(8)	7.4(3)
WS-X4008-DC=	400 W DC Power Supply for Catalyst 4000 series chassis	4.5(8)	7.4(3)
PWR-C45-1000AC=	1000 W AC Power Supply for Catalyst 4500 series chassis (Data only)	7.4(1)	7.4(3)
PWR-C45-1000AC/2=	1000 W AC Power Supply for Catalyst 4500 series chassis, Redundant (Data only)	7.4(1)	7.4(3)
PWR-C45-1300ACV=	1300 W AC Power Supply with in-line power for Catalyst 4500 series chassis	7.5(1)	7.6(16)
PWR-C45-1300ACV/2=	Redundant 1300 W AC Power Supply with in-line power for the Catalyst 4500 series chassis	7.5(1)	7.6(16)
PWR-C45-2800ACV=	2800 W AC Power Supply with in-line power for Catalyst 4500 series chassis	7.4(1)	7.4(3)
PWR-C45-2800ACV/2=	Redundant 2800 W AC Power Supply with in-line power for the Catalyst 4500 series chassis	7.4(1)	7.4(3)
PWR-C45-1400DC-P=	1400 W DC Power Supply with Integrated PEM for Catalyst 4500 series chassis	7.5(1)	7.6(16)
PWR-C45-1400DC-P/2=	Redundant 1400 W DC Power Supply with Integrated PEM for Catalyst 4500 series chassis	7.5(1)	7.6(16)

Release 7.*x* Orderable Software Images

Table 2 lists the software releases and applicable ordering information for Catalyst 4500 series supervisor engine software release 7.*x*.

Table 2 Release 7.x Orderable Software Image Matrix

Software Version	Filename	Orderable Product Number Flash Memory on System	Orderable Product Number Spare Upgrade (Floppy Media)
Supervisor Engine I and II			
7.6(17)	cat4000-k8.7-6-17.bin	SC4K-SUPK8-7.6.17	SC4K-SUPK8-7.6.17=
7.6(17) Secure Shell	cat4000-k9.7-6-17.bin	SC4K-SUPK9-7.6.17	SC4K-SUPK9-7.6.17=
7.6(16)	cat4000-k8.7-6-16.bin	SC4K-SUPK8-7.6.16	SC4K-SUPK8-7.6.16=
7.6(16) Secure Shell	cat4000-k9.7-6-16.bin	SC4K-SUPK9-7.6.16	SC4K-SUPK9-7.6.16=
7.6(15)	cat4000-k8.7-6-15.bin	SC4K-SUPK8-7.6.15	SC4K-SUPK8-7.6.15=
7.6(15) Secure Shell	cat4000-k9.7-6-15.bin	SC4K-SUPK9-7.6.15	SC4K-SUPK9-7.6.15=
7.6(14)	cat4000-k8.7-6-14.bin	SC4K-SUPK8-7.6.14	SC4K-SUPK8-7.6.14=
7.6(14) Secure Shell	cat4000-k9.7-6-14.bin	SC4K-SUPK9-7.6.14	SC4K-SUPK9-7.6.14=
7.6(13)	cat4000-k8.7-6-13.bin	SC4K-SUPK8-7.6.13	SC4K-SUPK8-7.6.13=
7.6(13) Secure Shell	cat4000-k9.7-6-13.bin	SC4K-SUPK9-7.6.13	SC4K-SUPK9-7.6.13=
7.6(12)	cat4000-k8.7-6-12.bin	SC4K-SUPK8-7.6.12	SC4K-SUPK8-7.6.12=
7.6(12) Secure Shell	cat4000-k9.7-6-12.bin	SC4K-SUPK9-7.6.12	SC4K-SUPK9-7.6.12=
7.6(11)	cat4000-k8.7-6-11.bin	SC4K-SUPK8-7.6.11	SC4K-SUPK8-7.6.11=
7.6(11) Secure Shell	cat4000-k9.7-6-11.bin	SC4K-SUPK9-7.6.11	SC4K-SUPK9-7.6.11=
7.6(10)	cat4000-k8.7-6-10.bin	SC4K-SUPK8-7.6.10	SC4K-SUPK8-7.6.10=
7.6(10) Secure Shell	cat4000-k9.7-6-10.bin	SC4K-SUPK9-7.6.10	SC4K-SUPK9-7.6.10=
7.6(9)	cat4000-k8.7-6-9.bin	SC4K-SUPK8-7.6.9	SC4K-SUPK8-7.6.9=
7.6(9) Secure Shell	cat4000-k9.7-6-9.bin	SC4K-SUPK9-7.6.9	SC4K-SUPK9-7.6.9=
7.6(8)	cat4000-k8.7-6-8.bin	SC4K-SUPK8-7.6.8	SC4K-SUPK8-7.6.8=
7.6(8) Secure Shell	cat4000-k9.7-6-8.bin	SC4K-SUPK9-7.6.8	SC4K-SUPK9-7.6.8=
7.6(7)	cat4000-k8.7-6-7.bin	SC4K-SUPK8-7.6.7	SC4K-SUPK8-7.6.7=
7.6(7) Secure Shell	cat4000-k9.7-6-7.bin	SC4K-SUPK9-7.6.7	SC4K-SUPK9-7.6.7=
7.6(6)	cat4000-k8.7-6-6.bin	SC4K-SUPK8-7.6.6	SC4K-SUPK8-7.6.6=
7.6(6) Secure Shell	cat4000-k9.7-6-6.bin	SC4K-SUPK9-7.6.6	SC4K-SUPK9-7.6.6=
7.6(5)	cat4000-k8.7-6-5.bin	SC4K-SUPK8-7.6.5	SC4K-SUPK8-7.6.5=
7.6(5) Secure Shell	cat4000-k9.7-6-5.bin	SC4K-SUPK9-7.6.5	SC4K-SUPK9-7.6.5=
7.6(4)	cat4000-k8.7-6-4.bin	SC4K-SUPK8-7.6.4	SC4K-SUPK8-7.6.4=
7.6(4) Secure Shell	cat4000-k9.7-6-4.bin	SC4K-SUPK9-7.6.4	SC4K-SUPK9-7.6.4=
7.6(3a)	cat4000-k8.7-6-3a.bin	SC4K-SUPK8-7.6.3a	SC4K-SUPK8-7.6.3a=
7.6(3a) Secure Shell	cat4000-k9.7-6-3a.bin	SC4K-SUPK9-7.6.3a	SC4K-SUPK9-7.6.3a=

Table 2 Release 7.x Orderable Software Image Matrix (continued)

Software Version	Filename	Orderable Product Number Flash Memory on System	Orderable Product Number Spare Upgrade (Floppy Media)
7.6(3)	cat4000-k8.7-6-3.bin	SC4K-SUPK8-7.6.3	SC4K-SUPK8-7.6.3=
7.6(2)	cat4000-k8.7-6-2.bin	SC4K-SUPK8-7.6.2	SC4K-SUPK8-7.6.2=
7.6(2) Secure Shell	cat4000-k9.7-6-2.bin	SC4K-SUPK9-7.6.2	SC4K-SUPK9-7.6.2=
7.6(1)	cat4000-k8.7-6-1.bin	SC4K-SUPK8-7.6.1	SC4K-SUPK8-7.6.1=
7.6(1) CiscoView	cat4000-cv.7-6-1.bin	SC4K-SUPCV-7.6.1	SC4K-SUPCV-7.6.1=
7.6(1) Secure Shell	cat4000-k9.7-6-1.bin	SC4K-SUPK9-7.6.1	SC4K-SUPK9-7.6.1=
7.5(1)	cat4000-k8.7-5-1.bin	SC4K-SUPK8-7.5.1	SC4K-SUPK8-7.5.1=
7.5(1) CiscoView	cat4000-cv.7-5-1.bin	SC4K-SUPCV-7.5.1	SC4K-SUPCV-7.5.1=
7.4(3)	cat4000-k8.7-4-3.bin	SC4K-SUPK8-7.4.3	SC4K-SUPK8-7.4.3=
7.4(3) CiscoView	cat4000-cv.7-4-3.bin	SC4K-SUPCV-7.4.3	SC4K-SUPCV-7.4.3=
7.4(3) Secure Shell	cat4000-k9.7-4-3.bin	SC4K-SUPK9-7.4.3	SC4K-SUPK9-7.4.3=
7.4(2)	cat4000-k8.7-4-2.bin	SC4K-SUPK8-7.4.2	SC4K-SUPK8-7.4.2=
7.4(2) CiscoView	cat4000-cv.7-4-2.bin	SC4K-SUPCV-7.4-2	SC4K-SUPCV-7.4.2=
7.4(2) Secure Shell	cat4000-k9.7-4-2.bin	SC4K-SUPK9-7.4-2	SC4K-SUPK9-7.4.2=
7.4(1)	cat4000-k8.7-4-1.bin	SC4K-SUPK8-7.4.1	SC4K-SUPK8-7.4.1=
7.4(1) Secure Shell	cat4000-k9.7-4-1.bin	SC4K-SUPK9-7.4.1	SC4K-SUPK9-7.4.1=
7.3(2)	cat4000-k8.7-3-2.bin	SC4K-SUPK8-7.3.2	SC4K-SUPK8-7.3.2=
7.3(2) CiscoView[1]	cat4000-cv.7-3-2.bin	SC4K-SUPCV-7.3-2	SC4K-SUPCV-7.3.2=
7.3(2) Secure Shell	cat4000-k9.7-3-2.bin	SC4K-SUPK9-7.3-2	SC4K-SUPK9-7.3.2=
7.3(1)	cat4000-k8.7-3-1.bin	SC4K-SUPK8-7.3.1	SC4K-SUPK8-7.3.1=
7.2(2) Secure Shell	cat4000-k9.7-2-2.bin	SC4K-SUPK9-7.2.2	SC4K-SUPK9-7.2.2=
7.2(2)	cat4000-k8.7-2-2.bin	SC4K-SUPK8-7.2.2	SC4K-SUPK8-7.2.2=
7.2(1)	cat4000-k8.7-2-1.bin	SC4K-SUPK8-7.2.1	SC4K-SUPK8-7.2.1=
7.2(1) CiscoView	cat4000-cv.7-2-1.bin	SC4K-SUPCV-7.2.1	SC4K-SUPCV-7.2.1=
7.2(1) Secure Shell	cat4000-k9.7-2-1.bin	SC4K-SUPK9-7.2.1	SC4K-SUPK9-7.2.1=
7.1(2a)	cat4000-k8.7-1-2a.bin	SC4K-SUPK8-7.1.2a	SC4K-SUPK8-7.1.2a=
7.1(2)	cat4000-k8.7-1-2.bin	SC4K-SUPK8-7.1.2	SC4K-SUPK8-7.1.2=
7.1(2) CiscoView	cat4000-cv.7-1-2.bin	SC4K-SUPCV-7.1.2	SC4K-SUPCV-7.1.2=
7.1(2) Secure Shell	cat4000-k9.7-1-2.bin	SC4K-SUPK9-7.1.2	SC4K-SUPK9-7.1.2=
7.1(1a)	cat4000-k8.7-1-1a.bin	SC4K-SUPK8-7.1.1a	SC4K-SUPK8-7.1.1a=
7.1(1)	cat4000-k8.7-1-1.bin	SC4K-SUPK8-7.1.1	SC4K-SUPK8-7.1.1=
7.1(1) CiscoView[2]	cat4000-cv.7-1-1.bin	SC4K-SUPCV-7.1.1	SC4K-SUPCV-7.1.1=
7.1(1) Secure Shell	cat4000-k9.7-1-1.bin	SC4K-SUPK9-7.1.1	SC4K-SUPK9-7.1.1=

1. The CiscoView application software in the CiscoView 7.3(1) image for the Catalyst 4500 series switch supports hardware and software features introduced in software releases 7.2(1) and 7.3(1).

2. The 7.1(1) CiscoView application software in the CiscoView image for the Catalyst 4500 series switch is the current 6.3(2) CiscoView version. The 7.1(1) CiscoView application software will be available at a later date. The new hardware and software features in release 7.1(1) are not supported by this CiscoView application until a new version of the CiscoView application becomes available. Release 7.1(1) CiscoView application which supports all new hardware/software features introduced in release 7.1(1) will become available at a later date.

New Features for Supervisor Engine Software Release 7.6

This section describes the new hardware and software features available in software release 7.6.

Hardware Features

No new hardware features have been added to software release 7.6.

Software Features

These software features are new to software release 7.6:

- Support for the following new and enhanced MIBs:
  - CISCO-ENVMON-MIB
  - CISCO-IP-IF-MIB
  - CISCO-PAE-MIB

New Features for Supervisor Engine Software Release 7.5

This section describes the new hardware and software features available in software release 7.5.

Hardware Features

These hardware features are new to software release 7.5:

- 1400 W DC power supply (PWR-C45-1400DC-P and PWR-C45-1400DC-P/2)

Software Features

These software features are new to software release 7.5:

- Local user authentication

  Local user authentication uses local user accounts and passwords that you create to validate the login attempts of local users rather than requiring a network authentication protocol such as RADIUS or TACACS+.

- Per-port unicast flood blocking

You can enable unicast flood blocking on any Ethernet port on a per-port basis. Unicast flood blocking allows you to drop unicast flood packets on an Ethernet port that has only one host connected to the port. All Ethernet ports on a switch are configured to allow unicast flooding; unicast flood blocking allows you to drop the unicast flood packets before they reach the port.

- Rapid PVST+

  Rapid PVST+ is the same as PVST+, although Rapid PVST+ utilizes a Rapid STP that is based on IEEE 802.1w instead of 802.1D. Rapid PVST+ uses the same configuration as PVST+ and you need only minimal extra configuration.

- RADIUS enhancement

  The framed-ip-address is now sent in the RADIUS authentication access-request packet.

- SNMP broadcast suppression enhancement
- SNMPv1 and SNMPv2c enhancements:
  - Setting multiple SNMP community strings
  - Clearing SNMP community strings
  - Specifying access numbers for hosts
  - Clearing IP addresses associated with access numbers
  - Specifying, displaying, and clearing an interface alias
- Support for these new and enhanced MIBs:
  - CISCO-FLASH-MIB enhancement
  - CISCO-VLAN-MEMBERSHIP-MIB enhancement
  - CISCO-VTP-MIB enhancement
  - RFC 2665 ETHERLIKE-MIB enhancement
  - RFC 2863 IF-MIB enhancement
  - RFC 2737 ENTIT-MIB enhancement
  - CISCO-STP-EXTENSION-MIB enhancement

New Features for Supervisor Engine Software Release 7.4

This section describes the new hardware and software features available in software release 7.4.

Hardware Features

These hardware features are new to software release 7.4:

- Catalyst 4503 chassis (WS-C4503)
- Catalyst 4506 chassis (WS-C4506)
- 1000 W power supply (PWR-C45-1000AC and PWR-C45-1000AC/2)
- 2800 W power supply (PWR-C45-2800ACV and PWR-C45-2800ACV/2)
- 1300 W variable power supply (PWR-C45-1300ACV and PWR-C45-1300ACV/2)

Software Features

These software feature is new to software release 7.4:

- Power management for the 1000 W, 1300 W, and 2800 W power supplies

  Support for redundant or combined power modes on the Catalyst 4500 series chassis with the 1000 W, 1300 W, and 2800 W power supplies.

New Features for Supervisor Engine Software Release 7.3

This section describes the new hardware and software features available in software release 7.3.

Hardware Features

No new hardware features have been added to software release 7.3.

Software Features

No new software features have been added to software release 7.3.

New Features for Supervisor Engine Software Release 7.2

This section describes the new hardware and software features available in software release 7.2.

Hardware Features

These hardware features are new to software release 7.2:

- 1000BASE-TX GBIC (WS-G5483)
- 1000BASE-X GBIC (CWDM-GBIC-1470, CWDM-GBIC-1490, CWDM-GBIC-1510, CWDM-GBIC-1530, CWDM-GBIC-1550, CWDM-GBIC-1570, CWDM-GBIC-1590, CWDM-GBIC-1610)

Software Features

These software features are new to software release 7.2:

- 4096 VLANs

  Catalyst 4500 series switches support 4096 VLANs in accordance with the IEEE 802.1Q standard.
- 802.1X VLAN assignment

  You can assign one or more switch ports to the VLAN.
- Authentication login lockout

The authentication login lockout feature is a lockout (delay) timer. It is configurable from the CLI and SNMP through the **set authentication login lockout** command. The configurable range is 30 to 600 seconds; setting the lockout time to zero (0) disables the feature.

If you are locked out at the console, the console does not allow you to log in during that lockout time. If you are locked out from a Telnet session, the connection closes when the limit is reached. Furthermore, the switch closes any subsequent access from that station during the lockout time and provides an appropriate notice.

- Errdisable reactivation

  You can manually prevent a port from being reactivated by setting the errdisable timeout for the port to disable; you can do this with the **set port errdisable-timeout mod/port disable** command.

- Ethernet link debounce timer feature

  The debounce time is the time a module's firmware waits before notifying the supervisor engine of a link change at the physical layer when a link goes down. If the link is up and then goes down and remains down for a time interval longer than the debounce time, the supervisor engine is notified. As soon as the link is up again, the timer is reset. If the link is down and then goes up, the supervisor engine is notified immediately. The debounce timer value is fixed in the supervisor engine depending upon the type of module being used. The link debounce feature can be enabled per port on Ethernet modules.

- VMPS server

  Catalyst 4500 series switches can function as VMPS servers.

New Features for Supervisor Engine Software Release 7.1

This section describes the new hardware and software features available in software release 7.1.

Hardware Features

This hardware feature is new to software release 7.1:

- 48-port Gigabit Ethernet 10/100/1000 switching module (WS-X4448-GB-rj45)

Software Features

These software features are new to software release 7.1:

- IEEE 802.1s Multiple Spanning Tree (MST) over 802.1Q VLAN trunks

  MST is an IEEE standard. 802.1s for MST is an amendment to 802.1Q. MST extends the 802.1w Rapid Spanning Tree (RST) algorithm to multiple spanning trees. This extension provides for both rapid convergence and load balancing in a VLAN environment. The MST protocol is still being developed and the MST feature for this release is based on a draft version of the IEEE standard. The protocol as implemented in this release is backward compatible with 802.1D STP, 802.1w, the rapid STP, and the Cisco PVST+ architecture.

- IEEE 802.3ad Link Aggregation Control Protocol (LACP)

LACP, which is defined in IEEE 802.3ad, allows Cisco switches to manage Ethernet channeling with devices that conform to 802.3ad. Prior to software release 7.1(1), Port Aggregation Control Protocol (PAgP) was available. PAgP is a Cisco-proprietary protocol that can be run only on Cisco switches and those switches released by licensed vendors.

- IEEE 802.1w rapid reconfiguration of spanning tree

  Provides for the rapid reconvergence of the spanning tree after the failure of any link in a bridged environment.

- PortFast on trunk ports

  Allows PortFast to be configured for trunk or channel ports. On link up, the port immediately transitions into spanning tree forwarding mode, bypassing listening and learning states, and bypassing DTP, PAgP, and 802.3ad protocols.

- MAC address notification

  The switch will report all learned and forgotten MAC addresses using SNMP traps.

- Multicast MAC address filtering

  Allows an administrator to filter incoming traffic and block specified multicast MAC addresses on specified ports, including IGMP control traffic and multicast data traffic. Multicast MAC address filtering is not dependent on VLANs.

- Support for the following MIBs:
  - CISCO-ENTITY-FRU-CONTROL-MIB
  - CISCO-ENVMON-MIB
  - IEEE8021-PAE-MIB

Open and Resolved Caveats in Software Release 7.6(17)

These sections describe the open and resolved caveats in supervisor engine software release 7.6(17):

- Open Caveats in Software Release 7.6(17), page 18
- Resolved Caveats in Software Release 7.6(17), page 18

Open Caveats in Software Release 7.6(17)

There are no open caveats in software release 7.6(17).

Resolved Caveats in Software Release 7.6(17)

These caveats are resolved in software release 7.6(17):

- The switch fails to return the complete Fully Qualified Domain Name (FQDN). The switch returns just the hostname and the domain is appended to the snmpset. When a management application reads the name it sees the hostname as being different then the running config. The mangement application then attempts to set the name by various means and starts a loop.

  Workaround: Specify the complete FQDN on the switch entering the **set system name nms-2948G.sys.etc** command and then on the NMS enter the **snmpwalk -c public nms-2948G sysName** command. This issue is resolved in release 7.6(17). (CSCsd37685)

- In rare cases, a Catalyst 4500 Supervisor Engine II might crash as a result of a memory allocation failure. (CSCsc77878)
- The primary and secondary associations are not saved in the configuration.

  Workaround: You need to map a switch port to the association using the **set pvlan primary_vlan** {*isolated_vlan* | *community_vlan*} *mod*/*port* command. (CSCsc02772)

Open and Resolved Caveats in Software Release 7.6(16)

These sections describe the open and resolved caveats in supervisor engine software release 7.6(16):

- Open Caveats in Software Release 7.6(16), page 19
- Resolved Caveats in Software Release 7.6(16), page 19

Open Caveats in Software Release 7.6(16)

There are no open caveats in software release 7.6(16).

Resolved Caveats in Software Release 7.6(16)

These caveats are resolved in software release 7.6(16):

- When you remove power from power supply 1 and enter the **show system** command, the switch displays the status of power supply 3 as fan failed and the system status as faulty. This occurs in the Catalyst 4006 chassis on Supervisor Engines running Software release 8.4(9) GLX or earlier software releases.

  Workaround: There is no workaround. (CSCsc76473)
- A Catalyst 4000 switch with a Supervisor Engine II (WS-X4013) running software release 7.6(11)GLX or higher reports connectivity problems, incrementing Interconnect VPD misses in the output of the **show health 1** command, and some devices not communicating with an end device.

  Workaround: Install a lesser version of the software. This problem is resolved in software release 7.6(16). (CSCsc25783)

Open and Resolved Caveats in Software Release 7.6(15)

These sections describe the open and resolved caveats in supervisor engine software release 7.6(15):

- Open Caveats in Software Release 7.6(15), page 19
- Resolved Caveats in Software Release 7.6(15), page 20

Open Caveats in Software Release 7.6(15)

There are no open caveats in software release 7.6(15).

Resolved Caveats in Software Release 7.6(15)

These caveats are resolved in software release 7.6(15):

- A Catalyst 4500 series switch may crash when running 802.1x and multiple ports receive a down link event followed by a link up. This problem is resolved in software release 7.6(15). (CSCsb60960)
- Under very rare and undetermined conditions, you might experience a condition in which the CAM aging time cannot be changed from the default value of 300 seconds. This lock condition is possibly triggered by a spanning tree topology change at the same time the set cam agingtime vlan value command is entered. The lock condition might also be the result of migrating from PVST+ to Rapid PVST+.

  Workaround: Reload the switch or revert momentarily to PVST+ and then back to Rapid PVST+. This problem is resolved in software release 7.6(15). (CSCef29999)

Open and Resolved Caveats in Software Release 7.6(14)

These sections describe the open and resolved caveats in supervisor engine software release 7.6(14):

- Open Caveats in Software Release 7.6(14), page 20
- Resolved Caveats in Software Release 7.6(14), page 20

Open Caveats in Software Release 7.6(14)

There are no open caveats in software release 7.6(14).

Resolved Caveats in Software Release 7.6(14)

These caveats are resolved in software release 7.6(14):

- Not all MST topology change events (TCs) are counted in the **show spantree** *mod/port* **mst** *instance* command output. The TCs are needed to determine the source and track the count of topology changes to troubleshoot excessive flooding. This problem is resolved in software release 7.6(14). (CSCsb11469)

Open and Resolved Caveats in Software Release 7.6(13)

These sections describe the open and resolved caveats in supervisor engine software release 7.6(13):

- Open Caveats in Software Release 7.6(13), page 20
- Resolved Caveats in Software Release 7.6(13), page 21

Open Caveats in Software Release 7.6(13)

There are no open caveats in software release 7.6(13).

Resolved Caveats in Software Release 7.6(13)

These caveats are resolved in software release 7.6(13):

- The time stamp displayed using the **show cam notification history** command reflects the SNMP sysUptime. The uptime is displayed as the number of 10-ms increments that have occurred since the system came up. This representation is not very user friendly when used within a CLI. This problem is resolved in software release 7.6(13). (CSCef96946)
- The 802.1X authentication state might be disturbed if the “multi-host” option is enabled and a second host sends an EAPOL frame.

  Workaround: Use the “multi-auth” mode or make sure only one device on the port sends an EAPOL frame. This problem is resolved in software release 7.6(13). (CSCeh24189)
- With 802.1X, an EAPOL logoff does not clear the EAPOL capable flag of a port when it receives the EAPOL logoff packet from an IP phone or supplicant. This problem is resolved in software release 7.6(13). (CSCeh65263)
- When an indirect failure is introduced in the spanning tree topology causing the message age timer to expire on the edge switches, UplinkFast does not get triggered if loop guard is configured. This problem is resolved in software release 7.6(13). (CSCeh19259)
- Netstat TCP displays negative values. This problem is resolved in software release 7.6(13). (CSCei21068)
- A switch running software release 7.6(8) will leak the memory over time. After the following message is displayed the switch will stop responding and will not switch traffic.

  ```
  2005 Feb 03 11:59:15 est -05:00 %SYS-3-SYS_MEMLOW:MCluster usage exceeded 90% 2005 Feb
  03 13:00:03 est -05:00 %SYS-3-SYS_MEMLOW:MCluster usage exceeded 90% 2005 Feb 03
  14:00:52 est -05:00 %SYS-3-SYS_MEMLOW:MCluster usage exceeded 90%
  ```

  Workaround: Do not to execute **show cam dynamic** command. If the switch stops switching traffic reboot the switch. This problem is resolved in software release 7.6(13). (CSCei14510)

Open and Resolved Caveats in Software Release 7.6(12)

These sections describe the open and resolved caveats in supervisor engine software release 7.6(12):

- Open Caveats in Software Release 7.6(12), page 21
- Resolved Caveats in Software Release 7.6(12), page 22

Open Caveats in Software Release 7.6(12)

There are no open caveats in software release 7.6(12).

Resolved Caveats in Software Release 7.6(12)

These caveats are resolved in software release 7.6(12):

- In rare occurrences, when a root switch is running Rapid PVST+ and a second switch is running in PVST+ mode, if a VLAN is added to the second switch and was preconfigured on the root switch, the second switch might receive malformed BPDUs from the root switch for that VLAN and the secondary root switch might not receive any BPDUs from the root switch on that particular VLAN. This behavior results in ports on the second switch going into forwarding mode causing a spanning tree loop. The loop may cause high CPU utilization on these switches. This problem is seen only when adding a VLAN to a switch that is running in PVST+ mode and only if the VLAN had been preconfigured for quite some time on the root switch which is running Rapid PVST+.

  Workaround: Remove the VLAN from all switches, add it again to all switches, then reboot the root switch or the secondary root switch. This problem is resolved in software release 7.6(12). (CSCeh53054)

- Using 802.1X, simultaneous authentications might fail. This problem is resolved in software release 7.6(12). (CSCeh52596)

- A Catalyst 4000 switch with a Supervisor Engine II (WS-X4013) may experience high cpu on the "Packet Forwarding" process after you upgrade your software from software release 6.4(15), 7.6(11), or 8.4(5)GLX.

  Workaround: There is no workaround. This problem is resolved in software release 7.6(12). (CSCeh26223)

Open and Resolved Caveats in Software Release 7.6(11)

These sections describe the open and resolved caveats in supervisor engine software release 7.6(11):

- Open Caveats in Software Release 7.6(11), page 22
- Resolved Caveats in Software Release 7.6(11), page 22

Open Caveats in Software Release 7.6(11)

There are no open caveats in software release 7.6(11).

Resolved Caveats in Software Release 7.6(11)

These caveats are resolved in software release 7.6(11):

- A WS-X4148-RJ45V auto-negotiates to 10-full when connected to computers with certain models of Intel Pro 1000 MT NIC card.

  Workaround: There is no workaround. his problem is resolved in software release 7.6(11). (CSCeg79650)

- A Catalyst 4500 series switch with a WS-X4448-GB-RJ45 module that includes 10/half hardcoded ports might display as connected, even if there is no cable connected to the port. This problem is resolved in software release 7.6(11). (CSCef43904)

- Currently, all dynamically learned secured mac-addresses are now stored in a context file. This problem is resolved in software release 7.6(11). (CSCef89420)

- In rare conditions Dot1x authenitication may cause a switch to reset. This problem is resolved in software release 7.6(11). (CSCeg36465)
- A Catalyst 4000 switch with a Supervisor Engine 2, configured with switch acceleration, reloads unexpectedly when the whichgigaport 1/1 or whichgigaport 1/2 hidden command is executed. This problem is resolved in software release 7.6(11). (CSCeg49479)
- The MIB object “snmpEngineTime” does not report the correct value if the SNMP engine has been active for more than 496 days. This problem is resolved in software release 7.6(11). (CSCeg61577)
- With a Supervisor Engine 2/MSFC2, a MST BPDU might not be generated when a blocking port forms a channel and moves to forwarding state. This behavior results in the CAM table not being flushed at the other end of the link which causes a communication loss. This problem is resolved in software release 7.6(11). (CSCee08366)
- You might experience a problem with an SSH login. The login prompt appears and you enter your login name and get a password login prompt. After entering the password, there is no reply; you see a blank line and pressing Enter again does nothing. If you try to enter a command, there is no echo on the screen *but* the output from the command is displayed on the screen. This problem is not affecting the ability of the switch to function correctly. Once the problem happens, it is continuous. Logging off and back on does not clear the problem. You must reboot the switch to clear the problem. If you attempt an SSH login on an affected switch and it fails, you can immediately do an SSH login to an unaffected switch from the same session without a problem. This problem is resolved in software release 7.6(11). (CSCef54438)
- If a port goes up and down, you might see a port security failure. If port security is enabled on the port, if the port goes up and down during the programming of the secure MAC address, you will lose connectivity. This problem is resolved in software release 7.6(11). (CSCef06707)
- You might see a VTP pruning failure with spanning tree PortFast enabled. This problem is resolved in software release 7.6(11). (CSCef86022)

Open and Resolved Caveats in Software Release 7.6(10)

These sections describe the open and resolved caveats in supervisor engine software release 7.6(10):

- Open Caveats in Software Release 7.6(10), page 23
- Resolved Caveats in Software Release 7.6(10), page 23

Open Caveats in Software Release 7.6(10)

There are no open caveats in software release 7.6(10).

Resolved Caveats in Software Release 7.6(10)

These caveats are resolved in software release 7.6(10):

- A Catalyst 4500 series switch with a WS-X4448-GB-RJ45 module that includes 10/half hardcoded ports might display as connected, even if there is no cable connected to the port. This problem is resolved in software release 7.6(10). (CSCef43904)

- A Catalyst 2980G switch might not prune VLANs as expected in a trunk when bouncing the trunk.

  Workaround: Disable VTP Prunning. This problem is resolved in software release 7.6(10). (CSCef20698)

- When you use the scheduled reset feature, the associated process (scheduleReset) might report several dynamic memory allocations in the **show memuse** command output, while the **show proc mem** command would not report any memory allocated or freed. This problem is resolved in software release 7.6(10). (CSCef50204)

- Your switch might crash if two SSH clients try to connect to the switch at the same time.This problem is resolved in software release 7.6(10). (CSCef60473)

- A switch can crash with the following error:

  ```
  Exception 2: Tlb exception (load or fetch)" at epc =>gcc2_compiled.(+ 0) after decoded
  the crashdump.
  ```

  This problem is resolved in software release 7.6(10). (CSCef65161)

- The switch does not respond properly when the logout timer is set to 3 (**set logout** 3) if you are accessing the switch through a Telnet session and the screen is either holding the display at the “More” prompt, the “Enter Password” prompt, or the “Username” prompt. The logout timer is ignored during these conditions, allowing the connection to remain open beyond the configured logout timer setting. This problem is resolved in software release 7.6(10). (CSCef15158)

- The dot1dStpPortDesignatedPort MIB might return the wrong value as compared to the **show spantree statistics** *mod/port* command output. This problem is resolved in software release 7.6(10). (CSCef79667)

- The switch displays the following syslog message when the system is under a Denial of Service attack:

  ```
  TCP-2-TCP_MAXESTABLISHED:Possible TCP ACK attack. . Maximum established connection
  limit 64 reached. Will drop unused connection
  ```

  However, under some circumstances, the syslog might be generated when the system is not under attack. The system functionality is not affected. This problem is resolved in software release 7.6(10). (CSCef77162)

- When standard MST is used with Layer 2 protocol tunneling, there might be convergence issues at the remote customer end. This problem is resolved in software release 7.6(10). (CSCef73654)

Open and Resolved Caveats in Software Release 7.6(9)

These sections describe the open and resolved caveats in supervisor engine software release 7.6(9):

- Open Caveats in Software Release 7.6(9), page 24
- Resolved Caveats in Software Release 7.6(9), page 25

Open Caveats in Software Release 7.6(9)

These caveats are open in software release 7.6(9):

- A Catalyst 4500 series switch with a WS-X4448-GB-RJ45 module that includes 10/half hardcoded ports might display as connected, even if there is no cable connected to the port. (CSCef43904)

Resolved Caveats in Software Release 7.6(9)

These caveats are resolved in software release 7.6(9):

- After executing many show commands over and over for 6~9 hours, via a telnet session, the system tries to access an off-limits address, and reloads. This problem is resolved in software release 7.6(9). (CSCee45047)
- If a MAC address is configured as a “filtered” address right after the MAC address is learned but before the address is aged out, traffic will not get filtered or dropped.

  Workaround: Enter the **clear cam dynamic** command. This problem is resolved in software release 7.6(9). (CSCin78010)
- A Catalyst 4500 series switch might reboot abnormally with the following exception code:

  ```
  Cause : Exception 2: Tlb exception (load or fetch)
  ```

  This problem is resolved in software release 7.6(9). (CSCef08126)
- A switch running software release 8.3(1)GLX may fail because of an SRAM failure with the following epc values in the crashdump:

  ```
  epc 0x00000000100fdee4
  epc 0x00000000100fd590
  ```

  Workaround: Disable the SRAM online diagnostics using the **set test switch-memory disable** command. This problem is resolved in software release 7.6(9). (CSCee88146)
- A Catalyst 4500 series switch might reboot abnormally with the following exception code:

  ```
  Cause : Exception 2: Tlb exception (load or fetch)
  ```

  This problem is resolved in software release 7.6(9). (CSCef08126)
- The dot3StatsFrameTooLongs counter should not increment when the port is configured as a trunk port. This problem is resolved in software release 7.6(9). (CSCee94947)
- If you upgrade your switch from any software release 7.x or earlier releases to software release 8.x and later releases with the boot mode set to “text” and spanning tree set to “PVST+,” the spanning-tree mode changes to “Rapid PVST+.”

  Workaround: Change the boot mode to “binary” before performing the upgrade. This problem is resolved in software release 7.6(9). (CSCin75737)
- With MISTP enabled and the EtherChannel mode set to "ON," if you configure more than one EtherChannel and trunk in a short period of time, all of the newly configured channels might not join the trunk. With this configuration scenario, the problem has also been seen after the switch is reset. This problem is resolved in software release 7.6(9). (CSCee95922)
- There is a vulnerability in the Transmission Control Protocol (TCP) specification (RFC793). All Cisco products that contain TCP stack are susceptible to this vulnerability. This advisory is available at these URLs:
  - http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml

    This URL describes this vulnerability as it applies to Cisco products that run Cisco IOS software.
  - http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml

    This URL describes this vulnerability for products that do not run Cisco IOS software.

  This problem is resolved in software release 7.6(9). (CSCed32349)

- It might take an unusually long time for a trunk port to join an EtherChannel. This problem is resolved in software release 7.6(9). (CSCee95479)
- When running a K9 software image, the switch might crash when the SSH client tries to connect to the switch. This problem is resolved in software release 7.6(9). (CSCdz04272)

Open and Resolved Caveats in Software Release 7.6(8)

These sections describe the open and resolved caveats in supervisor engine software release 7.6(8):

- Open Caveats in Software Release 7.6(8), page 26
- Resolved Caveats in Software Release 7.6(8), page 26

Open Caveats in Software Release 7.6(8)

These caveats are open in software release 7.6(8):

- A Catalyst 4500 series switch might reboot abnormally with the following exception code:

  ```
  Cause : Exception 2: Tlb exception (load or fetch)
  ```

  (CSCef08126)

Resolved Caveats in Software Release 7.6(8)

These caveats are resolved in software release 7.6(8):

- When using dynamic VLANs, if the MAC address is in a different VLAN that moves around beind the IP phones, the IP phone may end up with a MAC address assigned to the wrong VLAN.

  Workaround: Disable and reenable the port. This problem is resolved in software release 7.6(8). (CSCee59071)
- If you repeatedly power cycle the switch, the power status displays “fan failed” even if it has not failed. This problem is resolved in software release 7.6(8). (CSCee10783)
- The Catalyst 4500 series Supervisor Engine II (WS-X4013=) may stop responding when you are using Catalyst software release 7.6(8). This problem is resolved in software release 7.6(8). (CSCee33665)
- When using the **set boot autoconfig bootflash:config.txt** command after resetting the switch, the IGMP filter might not be applied on some ports. This situation occurs only when using the auto-config set up.

  Workaround: Copy the configuration file to NVRAM using the **copy flash config** command. This problem is resolved in software release 7.6(8). (CSCee69962)
- A UNIX script might get stuck at the Telnet prompt.

  Workaround: Press **Enter** at the point the script gets stuck to start the script again. This problem is resolved in software release 7.6(8). (CSCeb69513)
- The value of dot1dStpPortDesignatedPort is not correct when queried from SNMP. This problem is resolved in software release 7.6(8). (CSCee94422)

- Disabling or enabling port negotiation does not work correctly if you specify more than a single port or single range of ports. For example, if you enter **set port negotiation** 3/1,3/5-6 **disable**, ports 1 through 6 are disabled. This problem is resolved in software release 7.6(8). (CSCee52831)
- Doing a minimal entry (entering only the first part of a command syntax): **set errdisable**, **set option**, and **show cdp port** *mod/port*, on the following commands results in either a missing key word or no error message. This problem is resolved in software release 7.6(8). (CSCed92864)
- If you have an EtherChannel configured across modules, the EtherChannel configuration might change after disabling PortFast, BPDU filter, and BPDU guard and then resetting the switch. This problem is resolved in software release 7.6(8). (CSCee67595)
- An SNMP query for cvbStpForwardingMap might return an invalid port state. This problem is not resolved by a power cycle, module reset, disabling and enabling the port, or swapping modules. This problem is resolved in software release 7.6(8). (CSCee58481)
- If the default community strings are cleared, community strings configured by entering the **set snmp community-ext** command do not work after resetting the switch. This problem is resolved in software release 7.6(8). (CSCee66094)
- With a Supervisor Engine 2, when ports are added to an EtherChannel one port at a time, the calculated value of a path cost might be incorrect. In some cases, the path cost value displayed with the **show spantree mistp-instance** command is correct, but the path cost value displayed with the **show spantree statistics** command might be incorrect. Miscalculated path cost values result in ports going into the blocked state and create spanning tree topology discrepancies. This problem with the MISTP path cost feature appears in all software releases up to and including release 6.4(10). This problem is resolved in software release 7.6(8). (CSCee82347)
- A switch running software release 7.6(7) and rapid spanning tree (the switch is not the root bridge), might log the following events in the syslog if it received a corrupt BPDU:

```
2001 Apr 07 23:40:16 %SPANTREE-2-LOOPGUARDUNBLOCK: Port 4/2 restored in MST instance 1
2001 Apr 07 23:40:28 %SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 4/2 in
MST instance 1. Moved to loop-inconsistent state
2001 Apr 07 23:40:28 %SPANTREE-2-LOOPGUARDUNBLOCK: Port 4/2 restored in MST instance 1
2001 Apr 07 23:40:42 %SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 4/2 in
MST instance 1. Moved to loop-inconsistent state
2001 Apr 07 23:40:42 %SPANTREE-2-LOOPGUARDUNBLOCK: Port 4/2 restored in MST instance 1
2001 Apr 07 23:40:59 %SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 4/2 in
MST instance 1. Moved to loop-inconsistent state
2001 Apr 07 23:40:59 %SPANTREE-2-LOOPGUARDUNBLOCK: Port 4/2 restored in MST instance 1
2001 Apr 07 23:41:13 %SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 4/2 in
MST instance 1. Moved to loop-inconsistent state
2001 Apr 07 23:41:13 %SPANTREE-2-LOOPGUARDUNBLOCK: Port 4/2 restored in MST instance 1
```

  These symptoms are usually seen when there is more than one MST instance configured. This problem is resolved in software release 7.6(8). (CSCee77039)
- In text configuration mode, with the switch configured to send a “cold start” trap when the switch is reloaded, the switch does not send the trap after a reload. This problem does not appear when the configuration mode is set to binary. This problem is resolved in software release 7.6(8). (CSCee81130)
- With UplinkFast enabled, invalid dummy multicast packets might be sent out from the switch, resulting in communication failure.

  Workaround: Clear the ARP cache. This problem is resolved in software release 7.6(8). (CSCee22626)

Open and Resolved Caveats in Software Release 7.6(7)

These sections describe the open and resolved caveats in supervisor engine software release 7.6(7):

- Open Caveats in Software Release 7.6(7), page 28
- Resolved Caveats in Software Release 7.6(7), page 28

Open Caveats in Software Release 7.6(7)

There are no open caveats in software release 7.6(7).

Resolved Caveats in Software Release 7.6(7)

These caveats are resolved in software release 7.6(7):

- Spanning tree does not block ports when you use a Balun cable with your switch. If you loop a port with a Balun cable or loopback adapter, spanning tree blocks the port initially. However, if a topology change occurs, the port is set to a forwarding state. This problem is resolved in software release 7.6(7). (CSCed84323)
- When you use Secure Shell (SSH) to connect to a Catalyst switch, the switch may reset.

  Workaround: There is no workaround. This problem is resolved in software release 6.4(10). (CSCed84727)
- When your switch has a Supervisor Engine II G and many (approximately 20) trunk ports, all the available CPU resources are consumed by the EthChnlConfig process when you enable all of the ports at the same time or reboot the switch. In addition, VTP pruning cannot send out periodic messages on time, which causes the neighbor port to prune all VLANs on this trunk. When the CPU resources return to normal, VTP pruning recovers on its own. This problem is resolved in software release 7.6(7). (CSCdu44453)
- On a switch running a cryptographic (k9) image, if the value of sshPublicKeySize is non-zero, the SNMP_THREAD process might have a memory leak when sshPublicKeySize is polled. This problem is resolved in software release 7.6(7). (CSCed95950)
- When you issue part of the following commands (**set errdisable**, **set option**, **show cdp port mod/port**) you are either missing a key word or there is no error message. This problem is resolved in software release 7.6(7). (CSCed92864)

Open and Resolved Caveats in Software Release 7.6(6)

These sections describe the open and resolved caveats in supervisor engine software release 7.6(6):

- Open Caveats in Software Release 7.6(6), page 28
- Resolved Caveats in Software Release 7.6(6), page 29

Open Caveats in Software Release 7.6(6)

There are no open caveats in software release 7.6(6).

Resolved Caveats in Software Release 7.6(6)

These caveats are resolved in software release 7.6(6):

- When a user logs in to a Catalyst 4500 series switch with TACACS authentication configured, you will be prompted for a username even if the TACACS server is unavailable. This prompt might confuse users who are not aware that the TACACS server is unavailable when they may try to enter in a valid username/password combination.

  Workaround: To successfully log in, enter any value as a username, and use the switch enable password as the password for authentication. This problem is resolved in software release 7.6(6). (CSCdz16477)

- When you start a Telnet session to the Catalyst switch using certain Telnet clients, the Catalyst switch prompt is not displayed until you press the **Enter** (return) key.

  Workaround: Press the **Enter** key to get to the Catalyst switch prompt. This problem is resolved in software release 7.6(6). (CSCed45576)

- When you have a VMPS database downloading to the switch (initiated by entering the **download vmps** command), the switch might crash during the "VMPS Download" process. This problem is due to the vmps-port-group field not being specified in the VMPS configuration file. This problem is resolved in software release 7.6(6). (CSCed43310)

- If you lower the maximum number of MAC addresses allowed on a port using the **set port security** *mod*/*port* **maximum** *num_of_mac* command, you cannot clear all the secured addresses from your configuration using the **clear port security all** command.

  Workaround: Raise the number of MAC addresses allowed to a higher value using the **set port security** *mod*/*port* **maximum** *num_of_mac* command, and then issue the **clear port security all** command. This problem is resolved in software release 7.6(6). (CSCin66276)

- A Catalyst 4000 series or Catalyst 4503 switch with Supervisor Engine I or II or a WS-x5410 module in a Catalyst 5500 switch does not send dummy multicast packets when UplinkFast operates after **no shutdown** command has been entered from the original root port. This condition results in lost communication because the switch does not clear the older MAC table on the root port. This problem is resolved in software release 7.6(6). (CSCec79652)

- Even though you are unable to configure a private VLAN on a dynamic port from the CLI, a dynamic port can be configured into a private VLAN when the port receives the information from a VMPS server. Private VLANs cannot be assigned to dynamic ports. This problem is resolved in software release 7.6(6). (CSCin62512)

- When you use the **clear cam** *mac_addr* command to clear an autolearned MAC address on a port-security enabled port from the static CAM, the port can be placed in an inconsistent state and may not allow the user to configure the same MAC address on another port. If the port continues to receive the MAC address, the MAC address appears in the dynamic CAM instead of the static CAM.

  Workaround: Do not use the **clear cam** *mac_addr* command on a secure port. If a port is in an inconsistent state, use the **clear port security** *mod/port* command to clear the MAC address from the CAM. This problem is resolved in software release 7.6(6). (CSCin60971)

Open and Resolved Caveats in Software Release 7.6(5)

These sections describe the open and resolved caveats in supervisor engine software release 7.6(5):

- Open Caveats in Software Release 7.6(5), page 30
- Resolved Caveats in Software Release 7.6(5), page 30

Open Caveats in Software Release 7.6(5)

These caveats are open in software release 7.6(5):

- When you use the **clear cam** *mac_addr* command to clear an auto-learned MAC address on a port-security enabled port from the static CAM, the port can be placed in an inconsistent state and may not allow the user to configure the same MAC address on another port. If the port continues to receive the MAC address, the MAC address appears in the dynamic CAM instead of the static CAM.

  Workaround: Do not use the **clear cam** *mac_addr* command on a secure port. If a port is in an inconsistent state, use the **clear port security** *mod/port* command to clear the MAC address from the CAM. (CSCin60971)

Resolved Caveats in Software Release 7.6(5)

These caveats are resolved in software release 7.6(5):

- Starting in software release 6.4(7), you may see this warning message on your console:

  ```
  2003 Dec 01 17:55:01 PST -07:00 %SYS-4-P2_WARN:1/Traffic from permanent host
  00:04:c1:82:5f:ff but seen on incorrect port 1/2
  ```

  In most cases, this message is caused by ARP requests from the switch being flooded back to itself by a neighbor. Since the source MAC address is the system MAC address, a console message is logged and the packet is dropped. This problem is resolved in software release 7.6(5). (CSCed13361)

- In rare cases, when you enable CGMP, the Catalyst 4500 series Supervisor Engine I or Supervisor Engine II may reload intermittently. There is no workaround. This problem is resolved in software release 7.6(5). (CSCec72380)

- The packet memory on a Catalyst 4000 series Supervisor Engine may go bad, resulting in data packets being sent out with an invalid CRC and being discarded by the link partner. Diagnostics have been added to identify the problem. Once the problem is identified, the switch automatically resets and comes back up in a “best-effort” mode. In “best-effort” mode, the affected packet buffers are removed from circulation, and log messages are generated every 30 minutes to warn about the failures. You should replace a supervisor engine with packet memory errors. This problem is resolved in software release 7.6(5). (CSCec78085)

- The MAC address does not clear from the static CAM when you enter the **clear cam static** command; the MAC address may be learned by both the static and dynamic CAMs.

  Workaround: Enter the **clear cam** command to delete the user-configured static MAC addresses from the static CAM. If the switch reaches a condition that the same MAC address is learned on dynamic and static CAM, enter the **clear port security** and **clear cam dynamic** commands to clear the MAC address from the dynamic CAM and reach a “consistent” state. This problem is resolved in software release 7.6(5). (CSCin61896)

- When you use the clear cam permanent command to clear a permanent CAM filter entry, the filter entry is not removed from the hardware tables and traffic is dropped. This problem is resolved in software release 7.6(5). (CSCed11672)
- You can configure the auto-configure feature for port security in software release 7.6(5). However, there is no support for port security autoconfigure in the Catalyst 4500 series platform code.

  Workaround: Do not enable the auto-configure command for port security. Instead, you can add secure MAC addresses using the **set port security** command. This problem is resolved in software release 7.6(5). (CSCed24331)

Open and Resolved Caveats in Software Release 7.6(4)

These sections describe the open and resolved caveats in supervisor engine software release 7.6(4):

- Open Caveats in Software Release 7.6(4), page 31
- Resolved Caveats in Software Release 7.6(4), page 31

Open Caveats in Software Release 7.6(4)

These caveats are open in software release 7.6(4):

- When you use the **clear cam** *mac_addr* command to clear an auto-learned MAC address on a port-security enabled port from the static CAM, the port can be placed in an inconsistent state and may not allow the user to configure the same MAC address on another port. If the port continues to receive the MAC address, the MAC address appears in the dynamic CAM instead of the static CAM.

  Workaround: Do not use the **clear cam** *mac_addr* command on a secure port. If a port is in an inconsistent state use the **clear port security** <*mod/port* command to clear the MAC address from the CAM. (CSCin60971)

Resolved Caveats in Software Release 7.6(4)

These caveats are resolved in software release 7.6(4):

- When you are running software release 7.5(1) or 7.6(1) on the Catalyst 4003 switches with a Supervisor Engine I and on the Catalyst 4003 switch with a Supervisor Engine II, the wrong value might display for the portSecurityLastSRcAddr when a link-down trap is sent for a security violation. This problem is resolved in software release 7.6(4). (CSCeb49723)
- When a switch receives a filtered CAM entry on a VLAN with port security enabled, the switch may shut down the port. This problem is resolved in software release 7.6(4). (CSCin51183)
- If you set the vmVlan to a value that is larger than 1023, an assert failure occurs. This problem is resolved in software release 7.6(4). (CSCeb67164)
- Communication is lost after 15 seconds when Uplinkfast and the root port come up after a switch over. This situation causes some data packets to leak through the unblocked port before the port can send out dummy multicast packets. If the leaked packets reach the distribution switch later than the dummy multicast packets, the packets are considered as valid and are not removed from the CAM table until the packets age out. This problem is resolved in software release 7.6(4). (CSCeb58149)

- On a Catalyst 2948G switch you may lose the SPAN configuration after changing from binary to text config mode.

  Workaround: Reenter SPAN configurations. This problem is resolved in software release 7.6(4). (CSCec17704)

- If you initiate a session on a Supervisor Engine to a WS-X4232-L3 module the session may not work after running for an unknown period of time. This situation occurs because of an incorrect adjacency in the Catalyst operating system side of the inband MAC address for the WS-4232-L3 module.

  Workaround: Establish a Telnet session with a Gigabit Ethernet 3 or Gigabit Ethernet 4 port (or a subinterface IP address) and reset the WS-X4232-L3 module to temporarily recover the problem. After you have recovered the session, you need to move the sc0 interface into a different VLAN to avoid this problem in the future. This problem is resolved in software release 7.6(4). (CSCdx30617)

- When configuring VMPS, you may run out of memory in some rare instances.

  Workaround: Change all dynamic memberships to static and then back to dynamic. This problem is resolved in software release 7.6(4). (CSCec29748)

- A Catalyst 4500 series switch with spanning tree disabled may forward 1Q-BPDU packets causing a downstream port to incorrectly block its ports.

  Workaround: Enable spanning tree using the **set spantree enable** command. This problem is resolved in software release 7.6(4). (CSCeb43406)

- Upgrading a Catalyst 4500 series switch to software Release 12.1(13)EW can cause a problem with the WS-X4148-RJ45V Power over Ethernet (PoE) module.

  Workaround: Turn off autonegotiation using the **set port speed** command. This problem is resolved in software release 7.6(4). (CSCec67534)

- After upgrading a Catalyst 4500 series switch from software release 6.3(3) to software release 7.6(1), you cannot configure logging-level COPS. This problem is resolved in software release 7.6(4). (CSCec37831)

Open and Resolved Caveats in Software Release 7.6(3a)

These sections describe the open and resolved caveats in supervisor engine software release 7.6(3a):

- Open Caveats in Software Release 7.6(3a), page 32
- Resolved Caveats in Software Release 7.6(3a), page 33

Open Caveats in Software Release 7.6(3a)

These caveats are open in software release 7.6(3a):

- A Catalyst 4500 series switch with spanning tree disabled may forward 1Q-BPDU packets causing a downstream port to incorrectly block its ports.

  Workaround: Enable spanning tree using the **set spantree enable** command. (CSCeb43406)

- If a port with port security enabled receives a filtered CAM entry on a VLAN, the port may shut down.

  Workaround: There is no workaround. (CSCin51183)

Resolved Caveats in Software Release 7.6(3a)

These caveats are resolved in software release 7.6(3a):

- New vulnerabilities in the OpenSSH implementation for SSH servers have been announced.

  An affected network device, running an SSH server based on the OpenSSH implementation, may be vulnerable to a Denial of Service (DoS) attack when an exploit script is repeatedly executed against the same device. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20030917-openssh.shtml.

  This problem is resolved in software release 7.6(3a). (CSCec33092)

Open and Resolved Caveats in Software Release 7.6(3)

These sections describe the open and resolved caveats in supervisor engine software release 7.6(3):

- Open Caveats in Software Release 7.6(3), page 33
- Resolved Caveats in Software Release 7.6(3), page 33

Open Caveats in Software Release 7.6(3)

These caveats are open in software release 7.6(3):

- A Catalyst 4500 series switch with spanning tree disabled may forward 1Q-BPDU packets causing a downstream port to incorrectly block its ports.

  Workaround: Enable spanning tree using the **set spantree enable** command. (CSCeb43406)

- If a port with port security enabled receives a filtered CAM entry on a VLAN, the port may shut down.

  Workaround: There is no workaround. (CSCin51183)

Resolved Caveats in Software Release 7.6(3)

These caveats are resolved in software release 7.6(3):

- There is a memory leak in the DVLAN_RECONF process when you run a heavy CPU load. This problem is resolved in software release 7.6(3). (CSCeb85102)
- If the switch receives packets with the system address set to the Sc0 MAC address, the port may shut down and the Sc0 interface may become inaccessible.

  Workaround: Reset the switch. (CSCeb84608)

- If the RIT patch cable that connects the workstation to a Type1A Balun is pulled out too quickly, the port moves directly from fwd to loopback (fwd) state. After the port detects its own BPDU, it transitions to the blocking state. The interval in which the port is looped back may also loopback the outgoing data traffic. If port security has been enabled, then data traffic will be secured on that port; incoming traffic from the original ports will be restricted.

  Workaround: To remove the secured MAC address on the secured port, configure the agetimer to a minimum value. After some time, the secured MAC address is automatically cleared from that port. This problem is resolved in software release 7.6(3). (CSCeb12104)

Open and Resolved Caveats in Software Release 7.6(2)

These sections describe the open and resolved caveats in supervisor engine software release 7.6(2):

- Open Caveats in Software Release 7.6(2), page 34
- Resolved Caveats in Software Release 7.6(2), page 34

Open Caveats in Software Release 7.6(2)

These caveats are open in software release 7.6(2):

- If the RIT patch cable that connects the workstation to a Type1A Balun is pulled out too quickly, the port moves directly from fwd to loopback (fwd) state. After the port detects its own BPDU, it transitions to the blocking state. The interval in which the port is looped back may also loopback the outgoing data traffic. If port security has been enabled, then data traffic will be secured on that port; incoming traffic from the original ports will be restricted.

  Workaround: To remove the secured MAC address on the secured port, configure the agetimer to a minimum value. After some time, the secured MAC address is automatically cleared from that port. (CSCeb12104)

Resolved Caveats in Software Release 7.6(2)

These caveats are resolved in software release 7.6(2):

- The lower level ground start (gs) code contains two tables: port security and CAM. When the ageout timer expired, the autolearned MAC was cleaned from the security table but not from the CAM table. This situation resulted in a security violation.

  Workaround: Delete the MAC address from the gs CAM table and the security table during ageout. This problem is resolved in software release 7.6(2). (CSCeb27176)

- When configured as a VMPS client, a switch may reset upon receiving multiple MAC addresses on a dynamic port.

  Workaround: Downgrade the software to an image that does not have the fix for CSCea5001. This problem is resolved in software release 7.6(2). (CSCin43958)

- After you reboot a Catalyst 4500 series switch with an upgraded image and enable VMPS, the ports that are configured for dynamic VLAN assignment may not have connectivity.

  Workaround: Physically disconnect and reconnect the cable to the port. This problem is resolved in software release 7.6(2). (CSCea08895)

- A Catalyst 4006 switch with port channels enabled on the supervisor engine trunk can have a communication failure between interVLANs.

  Workaround: There is no workaround. This problem is resolved in software release 7.6(2). (CSCdz66547)

- When you enter the **show cam dynamic vlanid** command, the message “Unable to contact module x” displays and VMPS does not work.

  Workaround: There is no workaround. This problem is resolved in software release 7.6(2). (CSCea69221)

- Dynamic VLANs are not always updated on the switch when the incoming SA changes.

  Workaround: There is no workaround. This problem is resolved in software release 7.6(2). (CSCea50001)

- If you enable port security and MAC address learning on a switch, when the port sees a MAC address that contains all zeros, the port is disabled and there is no “Last-Src-Addr.”

  Workaround: Reenable the port. This problem is resolved in software release 7.6(2). (CSCea89001)

- Disabling 802.1X does not work for single authentication and multiple host modes.

  Workaround: No workaround is available. You can bring the port back to a normal state by using the **clear config all** command followed by resetting the switch. This problem is resolved in software release 7.6(2). (CSCin41724)

- There is a memory leak that increases the memory held by the console in 16 byte increments. This memory leak presents itself in one of two ways:

  – When you configure a community or isolated VLAN to a primary VLAN using the SNMP CLI.

  – Free memory reduces constantly and the memory held by the SptTimer and DTP_Rx process.

  You can use the **show proc mem** command to view the memory held by processes and verify if you have a memory leak.

  Workaround: There is no workaround. (CSCea91118)

Open and Resolved Caveats in Software Release 7.6(1)

These sections describe the open and resolved caveats in supervisor engine software release 7.6(1):

- Open Caveats in Software Release 7.6(1), page 35
- Resolved Caveats in Software Release 7.6(1), page 36

Open Caveats in Software Release 7.6(1)

These caveats are open in software release 7.6(1):

- A Catalyst 4500 series switch running in the access layer may display loop guard-inconsistent messages if a topology change occurs in corresponding designated switches that have a high number of spanning tree instances. The switch recovers on its own and does not cause a network outage.

  Workaround: There is no workaround. (CSCdz65842)

- After you reboot a Catalyst 4500 series switch with an upgraded image and enable VMPS, ports that are configured for dynamic VLAN assignment may not have connectivity.

  Workaround: Physically disconnect and reconnect the cable to the port. (CSCea08895)

- A Catalyst 4006 switch with port channels enabled on the supervisor engine trunk can have a communication failure between interVLANs.

  Workaround: There is no workaround. (CSCdz66547)

- When you enter the **show cam dynamic vlanid** command, the message "Unable to contact module x" displays and VMPS does not work.

  Workaround: There is no workaround. (CSCea69221)

- Dynamic VLANs are not always updated on the switch when the incoming SA changes.

  Workaround: There is no workaround. (CSCea50001)

Resolved Caveats in Software Release 7.6(1)

These caveats are resolved in software release 7.6(1):

- When CGMP is enabled on a Catalyst 4500 series switch, IGMP global leave is not generated after a spanning tree topology change occurs in MST mode.

  Workaround: Switch to PVST+ or Rapid PVST+ mode. This problem is resolved in software release 7.6(1). (CSCdz50009)

- Moving a host from a secured port to an unsecured port causes a security violation.

  Workaround: There is no workaround. This problem is resolved in software release 7.6(1). (CSCea07450)

- Under certain conditions a switch may overwhelm the console with log messages for 4 to 5 minutes when BPDU guard and port security are enabled. The workaround is to disable console logging using the **set logging console disable** command. This problem is resolved in software release 7.6(1). (CSCdz70110)

- When a port receives a VLAN assignment from the RADIUS server and the port mode is set to multiple-hosts, the output of the **show por**t command may show the old VLAN. The feature works correctly, allowing multiple hosts.

  Workaround: Ignore the output of the **show port** command. The output of the **show spantree** command displays the correct port in the appropriate state. This problem is resolved in software release 7.6(1). (CSCin26149)

- A port with port security enabled is not included in the static CAM table when an MC receiver is on the port. When the host sends an IGMP join report to the MC router, the MC router sends a CGMP join to the switch but the switch does not add the host to the static CAM table.

  If there are no other hosts, the switch will flood the MC traffic and all hosts will receive the traffic. However, if just one host with port security disabled joins the group, only that host will show up in the static CAM table and all other hosts will stop receiving the MC traffic.

  Workaround: Disable either port security or CGMP on the switch. This problem is resolved in software release 7.6(1). (CSCdz89564)

- The multicast entry for a trunk port in a nondefault VLAN disappears when you configure permanent CAM entries on the trunk port for any VLAN other than the default VLAN and reboot the system.

  Workaround: Clear the permanent CAM and reconfigure the CAM entries. This problem is resolved in software release 7.6(1). (CSCea31013)

- If you enable PortFast and BPDU guard on a port, you should not connect that port to a switch. BPDU storms will occur if there is a loop on the switch, and you cannot shut down the CPU until the loop is removed.

  Workaround: Never introduce a loop to a switch that is not running spanning tree. Also, if you enable PortFast and BPDU guard on a port, you should not connect that port to a switch. This problem is resolved in software release 7.6(1). (CSCdz03594)

- When configuring the local-user authentication feature, you configure a username and password combination for each user. If the user logs in using Telnet, there is no problem. However, if the user logs in using Secure Shell (SSH), the username and password combination fails because you have to set the password with the **set password** command.

  Workaround: There is no workaround. This problem is resolved in software release 7.6(1). (CSCea21326)

- Software release 7.5(1) does not apply the 96-percent power efficiency of the 1400 W DC power supply for inline power devices. Therefore, the amount of inline power that is allocated by the 1400 DC power supply and tracked by the software will be underestimated by approximately 4 percent. For example, if the **show environment power** command indicates that 96 W has been allocated for inline power, in fact 100 W has been allocated by the 1400 W DC power supply.

  Workaround: There is no workaround. (CSCea36031)

- Your system may crash if you are running low on memory and you enabled VMPS change trap. This problem is resolved in software release 7.6(1).

  Workaround: There is no workaround. (CSCea40726)

- When you upgrade a Catalyst 4500 series switch with a Supervisor Engine I or a Catalyst 2948G switch from software release 4.5(x) to software release 7.5(1) or a later release, those ports that have the default configuration for port-channeling will experience connectivity problems.

  Workaround: Before you upgrade your system software, enter the **set port channel** *mod/port* **mode off** command on those ports that have default port channeling enabled. If you have already upgraded your system software, you should enter the **set port host** *mod/port* command. (CSCea18590)

- Supervisor Engine II may show the status of a Catalyst 4500 series gateway running 12.2(16.4)T2 as faulty. This problem is resolved in software release 7.6(1).

  Workaround: There is no workaround. (CSCin37385)

- Disabling 802.1x does not work for single authentication and multiple host modes. To disable 802.1x, use the **port-control force-authorized** and **clear dot1x configuration** commands.

  Workaround: No workaround is available. You must enter the **clear config all** command, and reset the switch to bring the port back to the normal state. (CSCin41724)

Open and Resolved Caveats in Software Release 7.5(1)

These sections describe the open and resolved caveats in supervisor engine software release 7.5(1):

- Open Caveats in Software Release 7.5(1), page 38
- Resolved Caveats in Software Release 7.5(1), page 38

Open Caveats in Software Release 7.5(1)

These caveats are open in software release 7.5(1):

- A Catalyst 4500 series switch running in the access layer may display loop guard-inconsistent messages if a topology change occurs in corresponding designated switches that have a high number of spanning tree instances. The switch recovers on its own and does not cause a network outage.

  Workaround: There is no workaround. (CSCdz65842)

- When a port receives a VLAN assignment from the RADIUS server and the port mode is set to multiple-hosts, the output of the **show por**t command may show the old VLAN. The feature works correctly, allowing multiple hosts.

  Workaround: Ignore the output of the **show port** command. The output of the **show spantree** command displays the correct port in the appropriate state. (CSCin26149)

- If you change the port control of an authorized 802.1X port from **auto** to **force-authorized**, the port may display incorrect VLAN information in the output of the **show port** command and an error might occur when you try to change the VLAN for the port.

  Workaround: Disable and enable the port after changing port-control from **auto** to **force-authorized**. (CSCin25709)

- When CGMP is enabled on a Catalyst 4500 series switch, IGMP global leave is not generated after a spanning tree topology change occurs in MST mode.

  Workaround: Switch to PVST+ or Rapid PVST+ mode. (CSCdz50009)

- The *ciscoMemoryPoolUsed* and *ciscoMemoryPoolFree* values may report incorrect values when compared to the output for the **show version** command. These values indicate that SNMP reports a greater use of NVRAM then normal.

  Workaround: There is no workaround. (CSCdz42968)

Resolved Caveats in Software Release 7.5(1)

These caveats are resolved in software release 7.5(1):

- When you enable port security on a multi-VLAN access port, voice traffic may be switched untagged. The switch may learn the MAC address for an IP phone in both the static CAM and dynamic CAM. There is no workaround.This problem is resolved in software release 7.5(1). (CSCin19097)

- When switch CPU utilization approaches zero, a Catalyst 4500 series switch may return an invalid, negative value for the *cpmCPUTotal5sec* and *cpmCPTotal1min* values. This problem is resolved in software release 7.5(1). (CSCdz42365)

- If a port shuts down due to security violation, this behavior may occur:
  - If an age timer is not set, learned MAC addresses become configured addresses.
  - If an age timer is set, learned MAC addresses are cleared.

  This problem is resolved in software release 7.5(1). (CSCin25101)
- If you use RADIUS authentication to log into your switch from the integrated CiscoView utility, CiscoView may send the RADIUS the user ID $enabl5$ instead of the user ID you entered. This problem is resolved in software release 7.5(1). (CSCdz18313)
- When the supervisor engine fails POST, the software only functions partially and only a few select tasks run. When this failure occurs, the system will not update the power supply information and the power supply status information will not be displayed by the **show system** and **show test** commands. (CSCdz71607)

Open and Resolved Caveats in Software Release 7.4(3)

These sections describe the open and resolved caveats in supervisor engine software release 7.4(3):

- Open Caveats in Software Release 7.4(3), page 39
- Resolved Caveats in Software Release 7.4(3), page 39

Open Caveats in Software Release 7.4(3)

This is the open caveat in software release 7.4(3):

- A Catalyst 4500 series switch running in the access layer may display loop guard-inconsistent messages if a topology change occurs in corresponding designated switches that have a high number of spanning tree instances. The switch recovers on its own and does not cause a network outage. (CSCdz65842)

Resolved Caveats in Software Release 7.4(3)

These caveats are resolved in software release 7.4(3):

- Under rare circumstances, a Catalyst 4500 series switch will receive a corrupted VTP packet with an invalid vlan_id, which causes the switch to crash. The switch will recover automatically. This problem is resolved in software release 7.4(3). (CSCdy60111)
- RSPAN fails when it is enabled on a Catalyst 4500 series switch and the WS-X4448-GB-RJ45 port is selected as the reflector port. This problem is resolved in software release 7.4(3). (CSCdy87385)

Open and Resolved Caveats in Software Release 7.4(2)

These sections describe the open and resolved caveats in supervisor engine software release 7.4(2):

- Open Caveats in Software Release 7.4(2), page 40
- Resolved Caveats in Software Release 7.4(2), page 40
- Resolved Caveats in NonEmbedded CiscoView, page 40

Open Caveats in Software Release 7.4(2)

This is the open caveat in software release 7.4(2):

- A Catalyst 4500 series switch running in the access layer may display loop guard-inconsistent messages if a topology change occurs in corresponding designated switches that have a high number of spanning tree instances. The switch recovers on its own and does not cause a network outage. (CSCdz65842)

Resolved Caveats in Software Release 7.4(2)

These caveats are resolved in software release 7.4(2):

- If a switch is in VTP client mode and the trunk port connecting to the VTP server is no longer a trunk port, ping failure or traffic disruption might occur. This problem applies to software release 7.4(1) and earlier releases. This problem is resolved in software release 7.4(2). (CSCdy13083)
- A destination SPAN port configured to capture trunk ports cannot capture IEEE 802.1Q tagged packets after a reboot. This problem is resolved in software release 7.4(2). (CSCdy22282)

Resolved Caveats in NonEmbedded CiscoView

These caveats are resolved in nonembedded CiscoView:

- When CiscoView is set to show a Catalyst 4006 switch with an RSM module, an error may occur during the refresh. If the IP address for the RSM module is not configured, CiscoView tries to query the default value 0.0.0.0 and shows the error message. (CSCdy25800)

Open and Resolved Caveats in Software Release 7.4(1)

These sections describe the open and resolved caveats in supervisor engine software release 7.4(1):

- Open Caveats in Software Release 7.4(1), page 40
- Resolved Caveats in Software Release 7.4(1), page 41

Open Caveats in Software Release 7.4(1)

These caveats are open in software release 7.4(1):

- A Catalyst 4500 series switch running in the access layer may display loop guard-inconsistent messages if a topology change occurs in corresponding designated switches that have a high number of spanning tree instances. The switch recovers on its own and does not cause a network outage. (CSCdz65842)
- If a switch is in VTP client mode and the trunk port connecting to the VTP server is no longer a trunk port, ping failure or traffic disruption might occur. This applies to software release 7.4(1) and earlier releases.

  Workaround: Make the switch a VTP server. (CSCdy13083)

Resolved Caveats in Software Release 7.4(1)

These caveats are resolved in software release 7.4(1):

- If a static MAC address is installed using port security, a flood-path can be installed instead of a unicast path. Port security automatically installs a static MAC address if there is a secure address configured on the port. This problem is resolved in software release 7.4(1). (CSCdy14154)
- The port security shutdown timer might not work as expected by not reenabling the shutdown ports on all modules on a Catalyst 4500 series switch fully populated with WS-X4148 modules. This problem is resolved in software release 7.4(1). (CSCdy01966)

Open and Resolved Caveats in Software Release 7.3(2)

These sections describe the open and resolved caveats in supervisor engine software release 7.3(2):

- Open Caveats in Software Release 7.3(2), page 41
- Resolved Caveats in Software Release 7.3(2), page 41

Open Caveats in Software Release 7.3(2)

These caveats are open in software release 7.3(2):

- A Catalyst 4500 series switch running in the access layer may display loop guard-inconsistent messages if a topology change occurs in corresponding designated switches that have a high number of spanning tree instances. The switch recovers on its own and does not cause a network outage. (CSCdz65842)
- If a static MAC address is installed using the port security feature, a flood-path can be installed instead of a unicast path. The port security feature automatically installs a static MAC address if there is a secure address configured on the port. (CSCdy14154)

Resolved Caveats in Software Release 7.3(2)

There are no resolved caveats in software release 7.3(2).

Open and Resolved Caveats in Software Release 7.3(1)

These sections describe the open and resolved caveats in supervisor engine software release 7.3(1):

- Open Caveats in Software Release 7.3(1), page 42
- Resolved Caveats in Software Release 7.3(1), page 42
- Resolved Caveats in Software Release 7.3(1) CiscoView, page 43

Open Caveats in Software Release 7.3(1)

This is the open caveat in software release 7.3(1):

- A Catalyst 4500 series switch running in the access layer may display loop guard-inconsistent messages if a topology change occurs in corresponding designated switches that have a high number of spanning tree instances. The switch recovers on its own and does not cause a network outage. (CSCdz65842)

Resolved Caveats in Software Release 7.3(1)

These caveats are resolved in software release 7.3(1):

- When STP tries to send a SCP message to set CBL for a channel port, it queries the PAgP to get the corresponding physical ports. In some rare cases, the NMP gets a port that is removed from STP (also nontrunking) and sends an SCP message for that port resulting in native VLAN inconsistencies.

  Workaround: There is no workaround. This problem is resolved in software release 7.3(1). (CSCdw12370)

- When you use the **set trunk** command, **set udld enable 2/1-50** is also executed. If you then reset the switch, both commands are reflected in the **show config** output after reset.

  Workaround: There is no workaround. This problem is resolved in software release 7.3(1). (CSCdx12302)

- A Catalyst 4006 switch running a k9 image can crash if the switch acceleration is enabled and the switch is subsequently reset.

  Workaround: Disable switch acceleration when resetting the switch and enable it again after the switch has come up. This problem is resolved in software release 7.3(1). (CSCdw73412)

- The total number of all received errored packets (as represented in the CLI by the **show mac** command and its InLost counter) is not available through SNMP because the dot3StatsInternalMacRxErrs MIB is incorrect. This problem is resolved in software release 7.3(1). (CSCdw86025)

- If you use Merit Radius Server (a freeware application), and enter an invalid username to Telnet to a switch configured to use RADIUS authentication and a RADIUS server is available, the switch will reboot.

  Workaround: Use Cisco Secure Radius Server. This problem is resolved in software release 7.3(1). (CSCdx01532)

- An SNMP MIBwalk function with a community string in the format <*community string*>@<*vlan*> returns an incorrect value. This problem is resolved in software release 7.3(1). (CSCdx66883)

- In MST mode, the “set” and “get” actions on a channel port’s dot1dStpPortPriority object might not work properly. This problem is resolved in software release 7.3(1). (CSCdx23217)

- With spanning tree in MST mode, the stpxLongStpPortPathCost object cannot be set on any PAGP or LACP channels. This problem is resolved in software release 7.3(1). (CSCdx23200)

- The total number of all received error packets (as represented in the CLI by the **show mac** command and its InLost counter) is not available through SNMP because the dot3StatsInternalMacRxErrs MIB is incorrect. This problem is resolved in software release 7.3(1). (CSCdw86025)

- When the dot3adAggPortAttachedAggID SNMP MIB object value is queried, the returned value is wrong. As a result, applications that rely on the value returned from this object might fail. This problem impacts CiscoView. In CiscoView, these fields shows “N/A” when a port is configured for the LACP protocol on the Catalyst 6500 series and Catalyst 4500 series switches:
  - “Dot1Q Tunnel” field in Port -> Config -> Physical dialog
  - All fields in Port -> Config -> VTP Pruning dialog
  - When device is in MST Spanning tree mode, the “Preferred MST Instances” field in Port -> Config -> Spanning Tree -> MST Port Status dialog box does not work.

  This problem is resolved in software release 7.3(1). (CSCdw90927)
- When a reachable host and an unreachable host are configured as “syslog server” without a default gateway, only the first syslog message appears on the syslog server, no other syslog messages appear on the server. After clearing the unreachable host, messages that were not sent are sent to the reachable host all at once. The workaround is to clear the unreachable host from the configuration. This problem is resolved in software release 7.3(1). (CSCdx52404)

Resolved Caveats in Software Release 7.3(1) CiscoView

These caveats are resolved in software release 7.3(1) CiscoView:

- RSP LED is not supported on the Catalyst 2948G and 2980G devices. (CSCdw38266)
- 802.1X Authentication timer fields are available in the port level PAE dialog box. (CSCdw86044)
- When a device is set to MST Spanning Tree mode, the “Path Cost” and “Priority” fields in the Bridge Details dialog box cannot be set on a channeling port that is using PAgP or LACP. (CSCdx23217)

Open and Resolved Caveats in Software Release 7.2(2)

These sections describe the open and resolved caveats in supervisor engine software release 7.2(2):

- Open Caveats in Software Release 7.2(2), page 43
- Resolved Caveats in Software Release 7.2(2), page 44

Open Caveats in Software Release 7.2(2)

These caveats are open in software release 7.2(2):

- The total number of all received errored packets (as represented in the CLI by the **show mac** command and its InLost counter) is not available through SNMP because the dot3StatsInternalMacRxErrs MIB is incorrect. (CSCdw86025)
- When you use Merit Radius Server (a freeware application), and enter an invalid username to telnet to a switch configured to use RADIUS authentication and a RADIUS server is available, the switch will reboot.

  Workaround: Use Cisco Secure Radius Server. (CSCdx01532)
- A Catalyst 4500 series switch running in the access layer may display loop guard-inconsistent messages if a topology change occurs in the corresponding designated switches that have a high number of spanning tree instances. The switch recovers on its own and does not cause a network outage. (CSCdz65842)

Resolved Caveats in Software Release 7.2(2)

These caveats are resolved in software release 7.2(2):

- When the switch is running on one power supply, a faulty warning message is displayed in the output of the **show test** command, even when the switch is configured for 1+1 redundancy.

  Workaround: Ignore the warning. The switch needs only one power supply to operate. This problem is resolved in software release 7.2(2). (CSCdx19680)

- The Idledetect feature does not work on 10/100 ports of a Catalyst 2980G-A switch. If you attempt to configure Idledetect in the CLI, the switch ignores the configuration. This problem is resolved in software release 8.3(1)GLX. (CSCec79821)

- Ports on a Catalyst 2980G-A switch can stop receiving packets when connected to some hosts or ports with high ESD applied to them. This could happen in environments where cables are allowed to charge up to a high voltage. The ports will not receive any good packets. The Rx good packet count will not increase, and some error counters can increase when packets are received from neighboring hosts and switches. The symptoms are only temporary and will not damage your hardware. This problem is resolved in software releases greater than 7.2(1); however, it is disabled by default.

  To enable the fix, you must enable the idledetect feature, using the **set port idledetect** command. This feature is available only on Catalyst 2980G-A 10/100 ports. This problem is resolved in software release 7.2(2). (CSCdw37422)

- You might receive this faulty warning message:

  ```
  %SYS-2-PS_INSUFFICIENT:Insufficient power supplies operating, this system requires 2
  and only has 1
  ```

  Workaround: Ignore the warning, the switch needs only one power supply to operate. This problem is resolved in software release 7.2(2). (CSCdx22239)

- The Errdisable-timeout feature does not function properly on supervisor engine ports if the supervisor engine status is faulty. This problem can be caused by any system failure that leads to a faulty status on the supervisor engine, such as an unplugged power supply or bad fans. The problem, if caused by a minor fault in the system, has been resolved; if the system registers a major fault (Red console LED) the problem will still occur.

  Workaround: Verify that your supervisor engine does not display a faulty status and physically remove any unplugged power supplies from the chassis if you are using uplinks on your supervisor engine. (CSCdw75253)

Open and Resolved Caveats in Software Release 7.2(1)

These sections describe the open and resolved caveats in supervisor engine software release 7.2(1):

- Open Caveats in Software Release 7.2(1), page 45
- Resolved Caveats in Software Release 7.2(1), page 45

Open Caveats in Software Release 7.2(1)

These caveats are open in software release 7.2(1):

- A Catalyst 4500 series switch running in the access layer may display loop guard-inconsistent messages if a topology change occurs in corresponding designated switches that have a high number of spanning tree instances. The switch recovers on its own and does not cause a network outage. (CSCdz65842)
- When you use Merit Radius Server (a freeware application), and enter an invalid username to Telnet to a switch configured to use RADIUS authentication and a RADIUS server is available, the switch will reboot.

  Workaround: Use Cisco Secure Radius Server. (CSCdx01532)
- Ports on a Catalyst 2980G-A switch can stop receiving packets when connected to some hosts or ports with high ESD applied to them. This could happen in environments where cables are allowed to charge up to a high voltage. The ports will not receive any good packets. The Rx good packet count will not increase, and some error counters can increase when packets are received from neighboring hosts and switches. The symptoms are only temporary and will not damage your hardware. This problem is resolved in software releases later than 7.2(1); however, it is disabled by default.

  Workaround: Reset the switch. (CSCdw37422)
- ARP packets from an AIX server connected to the Catalyst 4000 with Gigabit EtherChannel (GEC) links are not received. This problem is intermittent. (CSCdv15018)

Resolved Caveats in Software Release 7.2(1)

These caveats are resolved in software release 7.2(1):

- CISCO-STACK-MIB SNMP controlled configuration download is not functioning correctly. This problem is resolved in software release 7.2(1). (CSCdx04874)
- When you are removing the fiber cable on a forwarding port, UplinkFast works fine and data traffic recovers after a few seconds; but when the whole module is disabled, it takes an average of 25 seconds for data traffic to recover. This problem is resolved in software release 7.2(1). (CSCdt41259)
- Two or more Catalyst 4003 switches configured for Remote Span (RSPAN) might experience a packet storm when one switch has active source and destination RSPAN ports, and the other has active source RSPAN ports.

  Workaround: Do not configure the local switch (switch with a destination port) with an RSPAN source port. This problem is resolved in software release 7.2(1). (CSCdx10678)
- Under certain circumstances, it is possible that the UplinkFast feature can cause high CPU utilization on a Catalyst 4500 series switch running MST or MISTP. If high CPU utilization does occur, the CPU utilization of the ufastMcast process will remain high until the switch is reloaded. This problem is resolved in software release 7.2(1). (CSCdu61791)
- The switch does not respond correctly to community strings that contain a “/”. This problem is resolved in software release 7.2(1). (CSCdx03088)

- When connected to a dynamic port, the IP phone cannot register with Cisco Call Manager.

  Workaround: To initially connect an IP phone, you must include the MAC address of the IP phone in the VMPS text file. If the IP phone is connected to your PC, you must assign the same VLAN for both the IP phone and the PC, or you might configure the IP phone to a fallback VLAN. Configuring the IP phone to a fallback VLAN will decrease the security level of your network. This problem is resolved in software release 7.2(1). (CSCdw71503)

- HP TopTool Remote Control Card v2.0 will join or leave the group approximately every 1 minute. This problem is resolved in software release 7.2(1). (CSCdw00897)

- A router in HSRP standby status is changed to active status. When status is restored, it does not go back to standby status from active status.

  Workaround: The router recovers if the interface on the HSRP standby side is set to shutdown or no shutdown. This problem is resolved in software release 7.2(1). (CSCdw32957)

- MST is not converging in networks with more than 200 VLANs, or in networks involving a Catalyst 4500 series switch running MST where a lot of topology changes are observed. This problem might happen if the switch is running software release 7.1(1) and the switch repeatedly flushes its dynamic CAM. This problem is resolved in software release 7.2(1). (CSCdw39902)

- The switch might crash if VTP is configured in client or server mode and connected to a Catalyst 4500 series switch with a Supervisor Engine III.

  Workaround: Configure VTP to use transparent mode. This problem is resolved in software release 7.2(1). (CSCdw41158)

- In certain configurations, the switch might drop IGMP reports before passing the reports to the router. If multicast functionality is based on CGMP, it will be affected.

  Workaround: Manually add a multicast static entry pointing to the CGMP router on the switch that is dropping IGMP reports. This problem is resolved in software release 7.2(1). (CSCdw60550)

- If you configure the switch with one trunk and 256 VLANs, the switch should handle 17,000 MAC addresses. Because the memory is shared, you cannot benchmark the maximum number of MAC address entries or VLANs. If the switch is configured with more than one trunk or more than 256 VLANs, you might see this error message:

  ```
  Failed to download VMPS configuration file.
  2002 Mar 01 16:25:20 %VMPS-2-NOMEM:Out of memory
  2002 Mar 01 16:25:20 %VMPS-2-DNLDFAIL:Download Failed. VMPS is now inactive
  ```

  The maximum size of the VMPS text configuration file that can be successfully downloaded by the VMPS server is 915,456 bytes. If the file is larger than 915,456 bytes, this error message is displayed:

  ```
  TFTP connection fail(-1).
  2002 Mar 01 16:14:34 %SYS-3-SUP_DNLDAREAEXCEED:Download aborted.
  File size larger than download buffer.
  Failed to download VMPS configuration file.
  2002 Mar 01 16:14:34 %VMPS-2-DOWNLOADFAIL2:Unable to download file vmps-mps
  2002 Mar 01 16:14:34 %VMPS-2-PREVCONF:VMPS is using the previous configuration
  ```

  This problem is resolved in software release 7.2(1). (CSCdw93962)

- MST is not converging in networks with more than 200 VLANs, or in networks involving a Catalyst 4500 series switch running MST where a lot of topology changes are observed. This problem might happen if the switch is running software release 7.1(1) and the switch repeatedly flushes its dynamic CAM. This problem is resolved in software release 7.2(1). (CSCdw39902)

- The switch might crash if VTP is configured in client or server mode and connected to a Catalyst 4500 series switch with a Supervisor Engine III.

  Workaround: Configure VTP to use transparent mode. This problem is resolved in software release 7.2(1). (CSCdw41158)

- In certain configurations, the switch might drop IGMP reports before passing the reports to the router. If multicast functionality is based on CGMP, it will be affected.

  Workaround: Manually add a multicast static entry pointing to the CGMP router on the switch that is dropping IGMP reports. This problem is resolved in software release 7.2(1). (CSCdw60550)

- You do not need to reload the switch to clear a faulty status for a supervisor engine. If the supervisor engine still shows up as faulty, there is another problem in the system, possibly a bad fan or a temperature alarm. This problem is resolved in software release 7.2(1). (CSCdw62053)

- On a Catalyst 2948G or 2980G switch, port negotiation or flow control commands are not saved in the configuration file. You can see this when you issue the **show config all** command. This does not affect the functionality of the switch, but if you reload the switch with a TFTP configuration file, the port negotiation and port flow-control configuration settings will be lost. The configuration remains intact in the NVRAM, and an ordinary reboot will not affect the configuration. This issue is not apparent on Catalyst 4500 series switches. This problem is resolved in software release 7.2(1). (CSCdw44268)

- You cannot configure the switch using the **set spantree root** command in software release 7.x. This problem is resolved in software release 7.2(1). (CSCdw76786)

Open and Resolved Caveats in Software Release 7.1(2a)

These sections describe the open and resolved caveats in supervisor engine software release 7.1(2a):

- Open Caveats in Software Release 7.1(2a), page 47
- Resolved Caveats in Software Release 7.1(2a), page 48

Open Caveats in Software Release 7.1(2a)

These caveats are open in software release 7.1(2a):

- A Catalyst 4500 series switch running in the access layer may display loop guard-inconsistent messages if a topology change occurs in corresponding designated switches that have a high number of spanning tree instances. The switch recovers on its own and does not cause a network outage. (CSCdz65842)

- When connecting NIC: SMC 8432BT with a DEC 21041-AA chipset on a PC Compaq Desktop 6xxxx to a 2980A-G switch at 10/HD, you might experience Align/FCS/Rcv-errors. (CSCdv79989)

- HP TopTool Remote Control Card v2.0 will join or leave the group approximately every 1 minute. (CSCdw00897)

- A router in HSRP standby status is changed to active status. When status is restored, it does not go back to standby status from active status.

  Workaround: The router recovers if the interface on the HSRP standby side is set to shutdown or no shutdown. (CSCdw32957)

- The switch does not send dummy frames with known dynamic MAC addresses if one of the uplinks is configured as GEC and it goes down. (CSCdw34521)

- ARP packets from an AIX server connected to the Catalyst 4000 with GEC links are not received. This problem is intermittent. (CSCdv15018)

Resolved Caveats in Software Release 7.1(2a)

These caveats are resolved in software release 7.1(2a):

- An error can occur with management protocol processing. Use the following URL for further information:

  http://www.cisco.com/cgi-bin/Bugtool/onebug.pl?bugid=CSCdw67458

  This problem is resolved in software release 7.1(2a). (CSCdw67458)

Open and Resolved Caveats in Software Release 7.1(2)

These sections describe the open and resolved caveats in supervisor engine software release 7.1(2):

- Open Caveats in Software Release 7.1(2), page 48
- Resolved Caveats in Software Release 7.1(2), page 49

Open Caveats in Software Release 7.1(2)

These caveats are open in software release 7.1(2):

- A Catalyst 4500 series switch running in the access layer may display loop guard-inconsistent messages if a topology change occurs in corresponding designated switches that have a high number of spanning tree instances. The switch recovers on its own and does not cause a network outage. (CSCdz65842)
- When connecting NIC: SMC 8432BT with a DEC 21041-AA chipset on a PC Compaq Desktop 6xxxx to a 2980A-G switch at 10/HD, you might experience Align/FCS/Rcv-errors. (CSCdv79989)
- HP TopTool Remote Control Card v2.0 will join or leave the group approximately every 1 minute. (CSCdw00897)
- The switch does not send dummy frames with known dynamic MAC addresses if one of the uplinks is configured as GEC and it goes down. (CSCdw34521)
- A router in HSRP standby status is changed to active status. When status is restored, it does not go back to standby status from active status.

  Workaround: The router recovers if the interface on the HSRP standby side is set to shutdown or no shutdown. (CSCdw32957)
- ARP packets from an AIX server connected to the Catalyst 4000 with GEC links are not received. This problem is intermittent. (CSCdv15018)

Resolved Caveats in Software Release 7.1(2)

These caveats are resolved in software release 7.1(2):

- A watchdog timer exception occurs because of an infinite loop in the cIgmpFilterTable. This problem is resolved in software release 7.1(2). (CSCdv19932)
- The sc0 interface does not work after you configure a private VLAN. This problem is resolved in software release 7.1(2). (CSCdv25263).
- Changing the spantree mode from PVST to MST.CAM table does not flush the table. This problem is resolved in software release 7.1(2). (CSCdv90770)
- When you access the system through an HTTP interface, an NMP exception occurs. This problem is resolved in software release 7.1(2). (CSCdw02887)
- VMPS does not work when a PC is moved between hubs. This problem is resolved in software release 7.1(2). (CSCdw23807)
- vlanPortIslOperStatus returns an incorrect trunking status. This problem is resolved in software release 7.1(2). (CSCdw24363)
- HSRP breaks when a CGMP leave is enabled. This problem is resolved in software release 7.1(2). (CSCdw31553)

Open and Resolved Caveats in Software Release 7.1(1a)

These sections describe the open and resolved caveats in supervisor engine software release 7.1(1a):

- Open Caveats in Software Release 7.1(1a), page 49
- Resolved Caveats in Software Release 7.1(1a), page 49

Open Caveats in Software Release 7.1(1a)

These caveats are open in software release 7.1(1a):

- A Catalyst 4500 series switch running in the access layer may display loop guard-inconsistent messages if a topology change occurs in corresponding designated switches that have a high number of spanning tree instances. The switch recovers on its own and does not cause a network outage. (CSCdz65842)
- A watchdog timer exception occurred because of an infinite loop in the CIGMPFilterTable. (CSCdv19932)

Resolved Caveats in Software Release 7.1(1a)

This section describes caveats resolved in software release 7.1(1a):

- An error can occur with management protocol processing. Use this URL for further information:

  http://www.cisco.com/cgi-bin/Bugtool/onebug.pl?bugid=CSCdw67458

  This problem is resolved in software release 7.1(2a). (CSCdw67458)

Open and Resolved Caveats in Software Release 7.1(1)

These sections describe the open and resolved caveats in supervisor engine software release 7.1(1):

- Open Caveats in Software Release 7.1(1), page 50
- Resolved Caveats in Software Release 7.1(1), page 50

Open Caveats in Software Release 7.1(1)

These caveats are open in software release 7.1(1):

- A Catalyst 4500 series switch running in the access layer may display loop guard-inconsistent messages if a topology change occurs in corresponding designated switches that have a high number of spanning tree instances. The switch recovers on its own and does not cause a network outage. (CSCdz65842)
- A watchdog timer exception occurred because of an infinite loop in the CIGMPFilterTable. (CSCdv19932)

Resolved Caveats in Software Release 7.1(1)

This section describes caveats resolved in software release 7.1(1):

- Creating an EtherChannel consisting of ports located on different modules might not work on Catalyst 4500 series switches.

  Workaround: Upgrade the switch software. This problem is resolved in software release 7.1(1). (CSCdv39598)

- If you have IP permit configured on your switch and you upgrade your switch software from a release of 5.4.2 or earlier to any release later than 5.4.2, you will lose your IP permit entries. However, the **ip permit enable** configuration will remain, and the switch might not be accessible from Telnet; the switch might still be accessible using other protocols, such as SNMP or SSH.

  Workaround: Upgrade the switch software. Before upgrading the switch software, back up the switch configuration and disable IP permit by using the **set ip permit disable** command. After you upgrade the software, enable the IP permit lists by using the **set ip permit enable** command, or restore the configuration from the backup you made before performing the software upgrade. This problem is resolved in software release 5.5(12). This problem is resolved in software release 7.1(1). (CSCdv81793)

- If you power off a switch, or the switch loses power during the ROMMON boot process, the system might fall back to the next image in the boot sequence. Repeating this process can lead to the system booting to the ROMMON CLI prompt, which will require manual intervention and connecting to the console serial port.

  Workaround: Do not power cycle switches before they finish booting, or you can fix the problem by upgrading the ROMMON. This problem is resolved in software release 7.1(1). (CSCdu45096)

Usage Guidelines, Restrictions, and Troubleshooting

This section provide usage guidelines, restrictions, and troubleshooting information for Catalyst 4500 series switch hardware and software.

- System and Supervisor Engine, page 51
- Modules and Switch Ports, page 52
- Spanning Tree, page 55
- VTP, VLANs, and VLAN Trunks, page 56
- EtherChannel, page 57
- SPAN, page 57
- Multicast, page 58
- MIBs, page 58
- Authentication, Authorization, and Accounting, page 58
- Nonembedded CiscoView, page 59

System and Supervisor Engine

This section contains usage guidelines, restrictions, and troubleshooting information that apply to the supervisor engine and to the switch at the system level:

- When connecting NIC: SMC 8432BT with a DEC 21041-AA chipset on a PC Compaq Desktop 6xxxx to a 2980A-G switch at 10/HD, you might experience Align/FCS/Rcv-errors.
- The Catalyst 4006 switch requires dual power supplies. Refer to the *Catalyst 4003 and 4006 Switch Installation Guide* for information about power requirements for the Catalyst 4500 series switches.
- In supervisor engine software release 5.2 and later, the **show config**, **write terminal**, and **copy config** commands return only the nondefault configuration (that is, only commands that change the default configuration are displayed). Use the **all** keyword to display both the default and nondefault configurations (for example, **show config all**).
- If you need to download configuration files to many switches in a network topology with redundant EtherChannel links, download the configuration at each switch manually using the **configure network** command. Otherwise, in some situations, a broadcast storm can occur.
- Under certain conditions, etherHistoryUtilization is not reported correctly if the counter value wraps between the two consecutive samples.

  Workaround: Reduce the sample interval.
- If your configuration produces thousands of CAM entries, ensure that your screen length is set to a value greater than 0 before entering the **show cam dynamic** command.
- The LrnDiscard counter (displayed by entering the **show mac** command) indicates the number of times a CAM entry is replaced with a newly learned address when the CAM table is full. The counter value is not maintained for each port; instead, the value is maintained for the entire switch.
- Although the **show spantree** command displays PortFast as enabled on a trunk port, spanning tree PortFast has no effect on trunk ports. Do not use the **set portfast** command on a trunk port. In addition, designating a port as a trunk port causes PortFast to be ignored for the port.
- The CLI command **show cam dynamic** and the SNMP query **getmany community@vlan dot1dTpFdbAddress** are sometimes not synchronized.

- The Port Name field in the output of the **show port** command displays only the first 18 characters of the port name. If you specify a port name that contains more than 18 characters the last characters will not be displayed in the output. (CSCed09784)
- If you attach a long cable (20 feet or longer) that is disconnected at the far end to the console port of a Catalyst 4500 series or Catalyst 2948G switch, then the resulting crosstalk on the serial line may prevent the switch from booting until you disconnect the cable from the switch or plug the cable into an active serial port (such as a serial port on a PC or a terminal server) at the remote end. (CSCdw69459 and CSCdr73326)
- The Catalyst 2948G switch may unexpectedly reset if a large number of ICMP redirect entries are learned by the switch. ICMP entries are stored in mbuf memory. When too many ICMP entries are learned, they use up crucial resources and cause the switch to reset.

  Workaround: Disable ICMP redirect learning by entering the **set icmp redirect disable** command. Configure static routes for the required destinations using the **set ip route** command. This problem is resolved in software release 7.6(5). (CSCed00225)

Caution If you upgrade from software release 7.6.4 to any higher 7.6.x release, with the auto-configure feature enabled, the feature remains enabled. Cisco Systems does not support the auto-configure feature on the Catalyst 4500 series platform. You can disable the auto-configure feature by entering the hidden **set port security auto-configure disable** command.

Modules and Switch Ports

This section contains usage guidelines, restrictions, and troubleshooting information that apply to modules and switch ports:

- Power over Ethernet modules do not support the Ethernet debounce timer. (CSCin52662)
- If a module fails to come online, reset the module by entering the **reset** *mod_num* command.
- This message indicates a potential port configuration error:

  ```
  2000 Feb 15 16:15:28 %SYS-4-P2_WARN: 1/Blocked queue on gigaport 5 ( 15 : 1 )
  ```

  If you receive this message, enter the command **show port counters** and check each port for excessive error frames, such as collisions, runts, and transmit errors.
- When hot inserting a module into a Catalyst 4500 series chassis, use the ejector levers on the front of the module to seat the backplane pins properly. Incorrectly inserting a module can cause unexpected behavior. For proper module installation instructions, refer to the *Catalyst 4003 and 4006 Switch Installation Guide*.
- When you replace a module (other than the supervisor engine) with a module of a different type, or when you insert a module (other than the supervisor engine) in an empty slot, entering the command **clear config** *mod_num* clears the module configuration information in the supervisor engine and obtains the correct spanning tree parameters.
- If a port fails the physical-medium-dependent (PMD) loopback test after the Catalyst 4500 series switch is reset (that is, if a port LED is flashing orange after a reset), you must reset the affected module.
- If the Catalyst 4500 series switch detects a port-duplex misconfiguration, the misconfigured switch port is disabled and placed in the errdisable state. Reconfigure the port-duplex setting and use the **set port enable** command to reenable the port.

- If you have a port whose speed is set to **auto** and is connected to another port whose speed is set to a fixed value, configure the port whose speed is set to a fixed value for half duplex, or you can configure both ports to a fixed-value port speed and full duplex.
- When you connect end stations (such as Windows 95, 98, or NT workstations) to Catalyst 4500 series 10/100-Mbps switch ports, we recommend this configuration:
  - Spanning tree PortFast enabled
  - Trunking off
  - Channeling off

  In supervisor engine software release 5.2 and later, you can use the **set port host** command to optimize the port configuration for host connections. This command automatically enables PortFast and sets the trunking and channeling modes to **off**.

  In software releases prior to release 5.2, you can optimize the port configuration for host connections as follows:
  - Use the **set spantree portfast** *mod_num/port_num* **enable** command to enable PortFast on a port.
  - Use the **set trunk** *mod_num/port_num* **off** command to disable trunking on a port.
  - Use the **set port channel** *port_list* **off** command to disable channeling on a port.

Note You must specify a valid port range when entering the **set port channel** command. You cannot specify a single port.

This example shows how to configure a port for end station connectivity using the **set port host** command:

```
Console> (enable) set port host 2/1

Warning: Spantree port fast start should only be enabled on ports connected
to a single host. Connecting hubs, concentrators, switches, bridges, etc. to
a fast start port can cause temporary spanning tree loops. Use with caution.

Spantree port 2/1 fast start enabled.
Port(s) 2/1 trunk mode set to off.
Port(s) 2/1 channel mode set to off.
Console> (enable)
```

This example shows how to manually configure a port for end station connectivity:

```
Console> (enable) set spantree portfast 2/2 enable

Warning: Spantree port fast start should only be enabled on ports connected
to a single host. Connecting hubs, concentrators, switches, bridges, etc. to
a fast start port can cause temporary spanning tree loops. Use with caution.

Spantree port 2/2 fast start enabled.
Console> (enable) set trunk 2/2 off
Port(s) 2/2 trunk mode set to off.
Console> (enable) set port channel 2/1-2 off
Port(s) 2/1-2 channel mode set to off.
Console> (enable)
```

- On Catalyst 4500 series modules that contain 10/100-Fast Ethernet ports, the Carri-Sen counter (in the output of the **show port** command) might erroneously show a value of 1, indicating an error occurred even though, in most cases, a carrier sense error did not occur.

- Do not plug an Ethernet cable into a serial port, because you will misconfigure your switch.
- These restrictions apply when configuring port security:
  - You cannot configure dynamic, static, or permanent CAM entries on a secure port.
  - When you enable port security on a port, any static or dynamic CAM entries associated with the port are cleared; any currently configured permanent CAM entries are treated as secure.
- If you configure a secure port to restrictive mode and a station is connected to the port whose MAC address is already configured as a secure MAC address on another port on the switch, the port in restrictive mode will shut down rather than restrict traffic from that station. For example, if you configure MAC-1 as the secure MAC address on port 2/1 and MAC-2 as the secure MAC address on port 2/2, and you then connect the station with MAC-1 to port 2/2 when port 2/2 is configured for restrictive mode, port 2/2 will shut down instead of restricting traffic from MAC-1.
- Do not enable protocol filtering on the switch if you have configured port security on any ports and set the violation mode to **restrict**. There is no restriction if the violation mode is set to **shutdown**; you can enable protocol filtering on the switch.
- When you connect a Catalyst 4500 series port that is set to autonegotiate an end station or another networking device, make sure that the other device also is configured for autonegotiation. If the other device is not set to autonegotiate, the Catalyst 4500 series autonegotiating port will remain in half-duplex mode, which can cause a duplex mismatch, resulting in packet loss, late collisions, and line errors on the link.
- Some ports on the Catalyst 4500 series oversubscribed Gigabit Ethernet modules do not reliably autonegotiate Ethernet operational modes with some Sun Gigabit Ethernet NICs. The 18-port server switching 1000BASE-X (GBIC) Gigabit Ethernet module (WS-X4418-GB) is affected.

  These Sun Gigabit Ethernet NICs are affected:
  - X1140A Sun Gigabit Ethernet Sbus Adapter 2.0
  - X1141A PCI Gigabit Ethernet PCI Adapter 2.0

  Workaround: Use this configuration:

Catalyst 4500 series Ports		**Sun Gigabit Ethernet NIC**	
Configuration	**Command**	**Configuration**	**Command**
Autonegotiation disabled	**set port negotiation** *mod_num/port_num* **disable**	Autonegotiation disabled	**ndd -set /dev/ge adv_1000autoneg_cap 0**
–	–	Half duplex off	**ndd -set /dev/ge adv_1000hdx_cap 0**
Send flow control on[1]	**set port flowcontrol** *mod_num/port_num* **send on**	Send flow control off	**ndd -set /dev/ge adv_pauseTX 0**
Receive flow control desired[1]	**set port flowcontrol** *mod_num/port_num* **receive desired**	Receive flow control on	**ndd -set /dev/gs adv_pauseRX 1**

1. Default setting

(CSCdm38405)

Spanning Tree

This section contains usage guidelines, restrictions, and troubleshooting information that apply to spanning tree:

- The Spanning Tree Protocol (STP) blocks certain ports to prevent physical loops in a redundant topology. On a blocked port, the Catalyst 4500 series switch receives spanning tree bridge protocol data units (BPDUs) periodically from the neighboring device. To configure the frequency with which BPDUs are received, enter the **set spantree hello** command (the default frequency is set to two seconds). If a Catalyst 4500 series switch does not receive a BPDU in the time defined by the **set spantree maxage** command (20 seconds by default), the blocked port transitions to the listening state, the learning state, and to the forwarding state. As it transitions, the switch waits for the time period specified by the **set spantree fwddelay** command (15 seconds by default) in each of these intermediate states. Therefore, a blocked spanning tree port moves into the forwarding state if it does not receive BPDUs from its neighbor within approximately 50 seconds.
- If the STP parameters are reduced in value, be sure that the number of STP instances is also reduced proportionally in order to avoid spanning tree loops in the network.
- You should configure a Catalyst series switch as the root for every VLAN, especially VLAN 1. In order to recover from an extended broadcast storm, Catalyst series switches must reset blocked ports. To ensure recovery, all Catalyst series switches in the network should reset blocked ports at the same time by sending synchronization packets on VLAN 1. A Catalyst series switch will not send synchronization packets unless it is the root bridge.
- Disabling spanning tree on the native VLAN of an IEEE 802.1Q trunk might cause spanning tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk. If you plan to disable spanning tree in an 802.1Q environment, disable it on every VLAN in the network to ensure that a loop-free topology exists.
- On your Catalyst 4500 series switch, be sure that the total number of logical ports across all instances of spanning tree for different VLANs does not exceed the number allowed for your supervisor engine.

  You can use the **show spantree summary** command and this formula to compute the sum of logical ports on the switch:

  (*number of trunks on the switch* × *number of active VLANs on those trunks*) + *number of nontrunking ports on the switch*

  The sum of all logical ports, as calculated with the formula above, should be less than or equal to the following:

  – 600 instances in PVST+ mode for the Catalyst 4500 series Supervisor Engine I and II
  – 9000 instances in MSTP mode for the Catalyst 4500 series Supervisor Engine I and II

Caution If you enable numerous memory-intensive features concurrently (such as VTP pruning, VMPS, EtherChannel, and RMON), or if there is switched data traffic on the management VLAN, the maximum number of supported logical ports is reduced.

Note Count each port in an EtherChannel port bundle independently (do not count the bundle as a single port).

- On a blocked spanning tree port, check the duplex configuration to ensure that the port duplex is set to the same type as the port of the neighboring device.

- On trunk ports, ensure that the trunk configuration is valid on both sides of the link.
- On a blocked spanning tree port, make sure that the Rcv-Frms and Rcv-Multi counters are incrementing continuously. If the Rcv-Frms counter stops incrementing, the port is not receiving any frames, including BPDUs. If the Rcv-Frms counter is incrementing but the Rcv-Multi counter is not, then this port is receiving nonmulticast frames but is not receiving any BPDUs.
- To monitor blocked spanning tree ports, use these commands:
  - Use the **show port** command to see if the port has registered many alignment, FCS, or any other type of line errors. If these errors are incrementing continuously, the port might drop input BPDUs.
  - Use the **show mac** command if the Inlost counter increments continuously or a port is losing input packets because of a lack of receive buffers. This problem can also cause the port to drop incoming BPDUs.
- On trunk ports, ensure that the duplex is set to full on both sides of the link to prevent collisions in heavy traffic conditions.
- Do not use spanning tree PortFast on a trunk port. Although the **show spantree** command displays PortFast as enabled on a trunk port, PortFast has no effect on such ports.

VTP, VLANs, and VLAN Trunks

This section contains usage guidelines, restrictions, and troubleshooting information that apply to VTP, VLANs, and VLAN trunks:

- The VLAN numbers are always ISL VLAN identifiers and not 802.1Q VLAN identifiers.
- A VTP transparent switch with no VTP domain name configured might not relay VTP requests received from VTP client and server switches. Therefore, VTP client and server switches might not synchronize if they are separated by a VTP transparent switch with no domain name configured.

  Workaround: Configure a VTP domain name on the VTP transparent switch.
- Although the Dynamic Trunk Protocol (DTP) is a point-to-point protocol, some internetworking devices might not forward DTP frames. To avoid connectivity problems, follow these guidelines:
  - For ports connected to non-Catalyst series devices in which trunking is not being used, configure trunk-capable Catalyst 4500 series switch ports to **off** by entering the **set trunk** *mod_num/port_num* **off** command.
  - When trunking to a Cisco router, use the **set trunk** *mod_num/port_num* **nonegotiate** command. The **nonegotiate** keyword transitions a link into trunking mode without sending DTP frames.
- With Cisco IOS Release 12.0, the Catalyst 8510 campus switch router (CSR) does not process untagged packets (packets on the native VLAN) received on an IEEE 802.1Q-trunked interface (all such packets are dropped). If you configure Catalyst 8510 CSR subinterfaces to a trunk using 802.1Q encapsulation, traffic cannot be carried successfully on the native VLAN for the trunk configured on a Catalyst 4500 series switch.

  Workaround: Create an unused VLAN and assign it as the native VLAN for the 802.1Q trunk on the Catalyst 4500 series switch. Verify the native VLAN assignment for the trunk using the **show trunk** command.

  This problem is tracked as a defect against the Catalyst 8510 CSR software. (CSCdk77676)

- IEEE 802.1Q trunks with several hundred active VLANs take a few minutes to become operational. The time increases with the number of VLANs on the trunk. During this time, you might see unexpected behavior, such as the console hanging or other ports not going into forwarding. After the trunks become operational, the unexpected behavior disappears and operation returns to normal. The operation remains normal as long as the trunks remain operational.

EtherChannel

This section contains usage guidelines, restrictions, and troubleshooting information that apply to Fast and Gigabit EtherChannel:

- With a large number of channels, trunks, or VLANs, or a change of channel configuration (for example, **off** to **auto**), or upon Fast EtherChannel module reboot, ports might take up to five minutes to form a channel and to participate in spanning tree. (During this interval, the port does not appear in **show spantree** command output.) If it takes more than ten minutes for a channel to form and appear on spanning tree, disable and reenable the ports. In addition, it might take up to two minutes to unbundle a channel after changing the channel mode.
- If a syslog message like "SPANTREE-2: Channel misconfig - *x/x-x* will be disabled" is displayed while running Fast EtherChannel, it indicates that one of the two ports is not configured correctly. We recommend that you reenable the ports by entering the **set port enable** command, and configure the two ports with one of these valid EtherChannel configurations.

Port Channel Mode	Valid Neighbor Port Channel Modes
desirable	**desirable** or **auto**
auto	**desirable**
on	**on**
off	**off**

SPAN

This section contains usage guidelines, restrictions, and troubleshooting information that apply to the Switched Port Analyzer (SPAN):

- By default, incoming traffic on the SPAN destination port is disabled. You can enable it using the **set span** command with the **inpkts enable** keywords. However, while the port receives traffic for its assigned VLAN, it does not participate in spanning tree for that VLAN. To avoid creating spanning tree loops with incoming traffic enabled, assign the SPAN destination port to an unused VLAN.
- A SPAN destination port receives flooded unicasts and broadcasts for the VLAN of the source SPAN port.
- A SPAN session cannot be configured through SNMP with the monitorGrp MIB. The SPAN configuration can be read from the monitorGrp MIB.

  Workaround: Use the PortCopyTable MIB to configure SPAN sessions through SNMP.

Multicast

This section contains usage guidelines, restrictions, and troubleshooting information that apply to multicast protocols and traffic on the switch:

- Because of a conflict with the Hot Standby Router Protocol (HSRP), Cisco Group Management Protocol (CGMP) leave processing is disabled by default. To enable CGMP leave processing, enter the **set cgmp leave enable** command.

  Note If both HSRP and CGMP leave processing are enabled, you might experience some unicast packet flooding.

- When CGMP leave processing is enabled, the Catalyst 4500 series switch learns router ports through PIM-v1, HSRP, and CGMP self-join messages. When CGMP leave processing is disabled, the Catalyst 4500 series switch learns router ports through CGMP self-join messages only.
- CGMP does not prune multicast traffic for any IP multicast address that maps into the MAC address range of 01-00-5E-00-00-00 to 01-00-5E-00-00-FF. The reserved IP multicast addresses, in the range 224.0.0.0 to 224.0.0.255, are used to forward local IP multicast traffic in a single Layer 3 hop.

MIBs

For information on MIBs, RMON groups, and traps, refer to the Cisco public MIB directory (http://www.cisco.com/public/mibs/). For information on the specific MIBs supported by the Catalyst 4500 series switches, refer to the Catalyst 4000 MIB Support List located at ftp://ftp.cisco.com/pub/mibs/supportlists/wsc4000/wsc4000-supportlist.html.

Authentication, Authorization, and Accounting

This section contains usage guidelines, restrictions, and troubleshooting information for authentication, authorization, and accounting (AAA):

- For login authentication, starting with software releases 5.5(15), 6.3(7), and 7.3(1), if you press the **Enter** key and then type your password, the ACS TACACS+ server will respond as if you are attempting to change your password. This behavior is related to CSCdx08395. Before the CSCdx08395 fix, the user privilege level was hard coded to 15 in the TACACS+ authentication request packet. With the CSCdx08395 fix, the user privilege level is set based on the privilege level at which the user is authenticated. For example, if a user attempts a login authentication, the privilege level is 1. If the user attempts an enable authentication, the privilege level is 15.

  The Cisco ACS TACACS+ server behaves differently when you press the **Enter** key and then type your password. When you press the **Enter** key and then type your password with the user priv-lvl hard coded to 15, the switch responds as if this is a login authentication as a regular password attempt. When you press the **Enter** key and then type your password with the user priv-lvl hard coded to 11, the switch responds as if you are changing your password. The latter case is a behavior consistent with TACACS+ enable authentication and Cisco IOS software handling when you press the **Enter** key and then type your password. (CSCdy35129)

Nonembedded CiscoView

This section contains usage guidelines, restrictions, and troubleshooting information that apply to nonembedded CiscoView:

- The supported client platforms, browsers, and Java Plug-in versions are as follows:

Client Platform	Web Browser	Java Plug-in
Solaris 2.7/2.8	Netscape Navigator 4.76, 4.77, 4.78, 4.79	Java Plug-in 1.3.0 (JRE 1.3.0) Java Plug-in 1.3.1 (JRE 1.3.1)
Windows 98 Windows NT 4.0 Windows 2000	Internet Explorer 5.5 Netscape Navigator 4.76, 4.77, 4.78, 4.79	Java Plug-in 1.3.0-C (JRE 1.3.0) Java Plug-in 1.3.1 (JRE 1.3.1)
HPUX 11.0	Netscape Navigator 4.77, 4.78, 4.79	Java Plug-in 1.2.2 (JRE 1.2.2) Java Plug-in 1.3.1 (JRE 1.3.1)
AIX 4.3.3	Netscape Navigator 4.77, 4.78, 4.79	Java Plug-in 1.3.0 (JRE 1.3.0) Java Plug-in 1.3.1 (JRE 1.3.1)

Note The Java Plug-in can be downloaded from http://www.cisco.com/cgi-bin/tablebuild.pl/cview-plugin

Note Java Plug-in versions 1.3.0_01 and 1.3.0_02 do not work with CiscoView.

Note Java Plug-in versions 1.3.1_01 and later are not supported by CiscoView.

- If the CiscoView chassis scroll bar does not appear, resize the browser window. Another workaround is to right-click on the chassis and select **Resize** to decrease the size of the chassis view.

  On Windows NT machines with Java Plug-in 1.3.0 installed and Netscape Navigator running, the CiscoView chassis scroll bar does not appear, even after you resize the window. To correct the problem, upgrade to Java Plug-in 1.3.1. (CSCdw58407)

- Nonembedded CiscoView does not work after you resize a browser window in Solaris. Make sure that you are using Netscape Communicator 4.7 from Sun Microsystems, not from Netscape.
- On Solaris machines that are running Netscape Navigator 4.77, 4.78, or 4.79, with Java Plug-in 1.3.1 installed, you might see a blank screen after launching CiscoView. (CSCdw13384)

  Follow these steps to correct the problem:

Step 1 Uninstall the current Java Plug-in from your machine.

Step 2 Download the Java Plug-in from this location and install it:

http://www.cisco.com/cgi-bin/tablebuild.pl/cview-plugin

Step 3 Clear the cache by entering this CLI command: **rm -rf ~/.netscape**

Step 4 Enter this CLI command: **export NPX_PLUGIN_PATH = /usr/j2se/jre/plugin/sparc/ns4**

Step 5 Launch Netscape Navigator.

Step 6 Select **Edit** > **Preferences**, and then click **Advanced** in the navigation tree.

Step 7 Make sure that the "Enable Java" check box is *not* selected.

Step 8 Specify the IP address of the device that you want to access and launch CiscoView. The Java console is displayed, but the chassis view does not appear.

Step 9 Select **Edit** > **Preferences**, and then click **Advanced** in the navigation tree.

Step 10 Select the "Enable Java" check box.

Step 11 Specify the IP address of the device that you want to access and launch CiscoView. Both the Java console and chassis view should display.

- If you are running Netscape Navigator with a Java Plug-in version that is earlier than version 1.3.0, you might get a blank screen when you launch CiscoView. (CSCdw59601)

  To correct the problem, download Java Plug-in 1.3.0 or later from this location: http://www.cisco.com/cgi-bin/tablebuild.pl/cview-plugin
- If your machine is running Windows 2000, Windows NT, or Windows 98 and the chassis view does not appear, you should disable the Java Plug-in's JAR caching feature, as follows:
  - For Java Plug-in 1.3.1:

    1) Select **Start** > **Settings** > **Control Panel** > **Java Plug-in 1.3.1**.

    2) Click the **Cache** tab.

    3) Click **Clear JAR Cache.**
  - For Java Plug-in 1.3.0:

    1) Select **Start** > **Settings** > **Control Panel** > **Java Plug-in**.

    2) Click the **Basic** tab.

    3) Make sure the "Cache JARs In Memory" check box is not selected.

    4) Click **Apply**.
- If your machine runs on the HP-UX platform, we recommend that you use the HP release of Netscape. The HP release of Netscape can be downloaded from this location: http://h30097.www3.hp.com/internet/comm479_form.html (CSCdw59617)
- CiscoView images take approximately 12 minutes to download from a TFTP server to a PCMCIA Flash memory card. (CSCdr14437)
- In the VLAN & Bridge dialog box (**Device** > **Configure** > **VLAN & Bridge**), deleting the primary VLAN after unbinding the secondary VLAN returns an error message. The workaround is to close and reopen the dialog box and then delete the primary VLAN.

  After binding a secondary VLAN to the primary VLAN, delete the primary VLAN and the following error message is displayed: "Set failed due to snmpRspGenErr for vtpVlanEditRowStatus.1.199." The workaround is to close and then reopen the dialog box. You should now see the correct error message: "The Primary is bounded ..." (CSCdt65530)
- Disabled WAN modules are placed in the power-down state. (CSCdw50083)
- The Carrier Alarm LED on WAN modules is not supported. (CSCdw50111)

- There is a problem when you highlight the MultiChannel DS3 Port Adapter in the WS-X6182-PA module, and then select **Configure > Interface**. The dialog box displays "n/a" or the incorrect values in every field. Also, if you select **Monitor > Interface,** the charts in the resulting dialog box do not get updated, and an error message is displayed in the status bar. (CSCdr39591)
- The LED labeled RPS is not supported on Catalyst 2948G and 2980G devices. (CSCdw38266)
- Daughter cards on the WS-X4604-GWY card are not supported. (CSCdw51541)
- Deleting the primary VLAN in the VLAN and Bridge dialog box after unbinding the secondary VLAN causes an error message to be displayed.

  Workaround: Close and reopen the VLAN and Bridge dialog box; delete the primary VLAN. (CSCdt65530)
- After binding a secondary VLAN to the primary VLAN, delete the primary VLAN. This error message is displayed:

  ```
  Set failed due to snmpRspGenErr for vtpVlanEditRowStatus1.199.
  ```

  Workaround: Close and reopen the VLAN and Bridge dialog box. The correct message displays. (CSCdt65530)
- Ports G1 and G2 on the WS-X4232-L3 card will always show the presence of GBIC modules. (CSCdr29617)
- 802.1X authentication timer fields are available in the port level PAE dialog box. (CSCdw86044)
- When a device is set to MST Spanning Tree mode, the path cost and priority fields in the Bridge Details dialog box cannot be set on a channeling port that is using PAGP or LACP. (CSCdx23200 and CSCdx23217)
- In the EtherChannel dialog box, when EtherChannel Operation Mode is changed from *pagpon* to either off or manual, click the Refresh button and the PAgP dialog box displays N/A for every field.

  Workaround: Close and reopen the EtherChannel dialog box. (CSCdw76309)

Software Documentation Updates for Release 7.1

This section describes caveats for the Catalyst 4500 series software release 7.1 documentation. These changes will be included in the next update to the documentation.

- Link Aggregation Control Protocol (LACP), which is defined in IEEE 802.3ad, allows Cisco switches to manage Ethernet channeling with devices that conform to the 802.3ad specification. Prior to software release 7.1(1), PAgP was available. PAgP is a Cisco-proprietary protocol that can be run only on Cisco switches and those switches released by licensed vendors.

Related Documentation

These documents are available for Catalyst 4500 series switches:

- *Catalyst 4000 Series Switch Installation Guide*
- *Catalyst 4500 Series Switch Installation Guide*
- *Catalyst 4912G Switch Installation Guide*
- *Catalyst 4500 Series, Catalyst 2948G, 2948G-GLX, and 2980 Switches Software Configuration Guide*

- *Layer 3 Switching Software Configuration Guide—Catalyst 5000 Family, 4000 Family, 2926G Series, and 2948G Switches*
- *Catalyst 4500 Series, Catalyst 2948G, 2948G-GLX, and Catalyst 2980 Switches Command Reference*
- *System Message Guide—Catalyst 6500 Series, Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980 Switches*
- *Troubleshooting Tips—Catalyst 5000 Family, 4000 Family, 2926G Series, and 2948G Switches*
- *Enterprise MIB User Quick Reference* (online only)

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Copyright © 2001—2006 Cisco Systems, Inc. All rights reserved.